Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Parliamentary Joint Committee on Intelligence and Security
© Commonwealth of Australia

ISBN 978-1-74366-969-3 (Printed Version)


This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia License.

The details of this licence are available on the Creative Commons website: http://creativecommons.org/licenses/by-nc-nd/3.0/au/.
Contents

Membership of the Committee ............................................................................................... v
Terms of reference .................................................................................................................. vii
Abbreviations ........................................................................................................................ ix
List of Recommendations ...................................................................................................... xi

The Report

1 The Report ........................................................................................................................... 1

Introduction .......................................................................................................................... 1

2018 Bill Review .................................................................................................................... 1

Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 ....................................................... 2

2019 Act Review ................................................................................................................... 2

Committee comment ............................................................................................................. 4

Matters identified by stakeholders for further consideration .............................................. 4

Statutory review and timing of the INSLM’s review ......................................................... 5

Operationalisation of the Act ............................................................................................. 6

Appendix A. Summary of evidence .................................................................................... 9

Appendix B. List of submissions ........................................................................................ 121
Membership of the Committee

Chair

Mr Andrew Hastie MP                 Canning, WA

Deputy Chair

Hon Anthony Byrne MP                Holt, VIC

Members

Senator the Hon Eric Abetz          LP, TAS
Senator David Bushby (until 21.1.2019) LP, TAS
Hon Mark Dreyfus QC, MP             Isaacs, VIC
Hon Dr Mike Kelly AM, MP            Eden-Monaro, NSW
Mr Julian Leeser MP                 Berowra, NSW
Senator Jenny McAllister            ALP, NSW
Senator Jim Molan AO, DSC           LP, NSW
Senator Amanda Stoker (from 12.2.2019) LP, QLD
Senator the Hon Penny Wong          ALP, SA
Mr Jason Wood MP                    La Trobe, VIC
Terms of Reference

On 6 December 2018, the Senate referred the operation of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 for inquiry and report by 3 April 2019.
## Abbreviations

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2018 Bill Review</td>
<td>Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018</td>
</tr>
<tr>
<td>2019 Act Review</td>
<td>Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018</td>
</tr>
<tr>
<td>Assistance and Access Act</td>
<td>Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018</td>
</tr>
<tr>
<td>Assistance and Access Bill</td>
<td>Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018</td>
</tr>
<tr>
<td>AFP</td>
<td>Australian Federal Police</td>
</tr>
<tr>
<td>ASD</td>
<td>Australian Signals Directorate</td>
</tr>
<tr>
<td>ASIO</td>
<td>Australian Security Intelligence Organisation</td>
</tr>
<tr>
<td>ASIS</td>
<td>Australian Secret Intelligence Service</td>
</tr>
<tr>
<td>IGIS</td>
<td>Inspector-General of Intelligence and Security</td>
</tr>
<tr>
<td>Industry assistance measures</td>
<td>Collective term for technical assistance requests, technical assistance notices and technical capability notices</td>
</tr>
<tr>
<td>INSLM</td>
<td>Independent National Security Legislation Monitor</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>TAN</td>
<td>Technical Assistance Notice</td>
</tr>
<tr>
<td>TAR</td>
<td>Technical Assistance Request</td>
</tr>
<tr>
<td>TCN</td>
<td>Technical Capability Notice</td>
</tr>
<tr>
<td>TIA Act</td>
<td><em>Telecommunications (Interception and Access) Act 1979</em></td>
</tr>
</tbody>
</table>
List of Recommendations

Recommendation 1

1.24 The Committee recommends that section 187N of the *Telecommunications (Interception and Access) Act 1979* be amended to require the Committee’s review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* by June 2020.

Recommendation 2

1.25 The Committee recommends that sufficient resources be made available to the Independent National Security Legislation Monitor to enable the review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, as referred by the Committee, and report by 1 March 2020.

Recommendation 3

1.31 The Committee recommends that the Government continues to ensure that the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman have sufficient resources to ensure that they can properly execute their additional responsibilities under the Assistance and Access Act.
1. The Report

Introduction

1.1 On 6 December 2018, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Assistance and Access Act) was referred to the Committee for inquiry and report by 3 April 2019. The referral formed part of a second reading amendment moved during Senate consideration of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (the Assistance and Access Bill).

1.2 The Committee adopted this review on 14 December 2019 (referred to in this report as the 2019 Act Review). The referral is a subsequent and separate review from that conducted by this Committee in 2018 on the Assistance and Access Bill (2018 Bill Review).

2018 Bill Review

1.3 On 20 September 2018, the Attorney-General referred the Assistance and Access Bill to the Committee for inquiry and report. The Committee subsequently launched a detailed review of the legislation which attracted over 100 submissions from industry and members of the public, involved five public hearings and multiple private hearings and classified briefings.

1.4 At the end of 2018 the Committee agreed to expedite its consideration of the Bill following Government advice that the legislation was critical to assist agencies’ response to a heightened national security environment over the Christmas/New Year period. In recognition of this advice and the imperative to pass the Assistance and Access Bill before the conclusion of sittings for 2018, the Committee tabled a brief report recommending a series of
amendments to respond to the most pressing issues raised during the 2018 Bill Review.

Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

1.5 The Committee’s Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the 2018 Report) was tabled on 5 December 2018. It contained 17 recommendations for amendment or other action by Government, primarily aimed at improving the efficacy and oversight of the industry assistance measures provided for in Schedule 1 of the Bill.

1.6 The tight reporting timeframe prevented the Committee from clarifying the intent and objectives of its recommendations through its long-standing practice of detailed Committee comments. The expedited consideration also precluded the Committee from incorporating a detailed presentation of the evidence informing its recommendations.

1.7 In response to the Committee’s report, amendments to the Bill were introduced and passed by the Parliament on 6 December 2018, the final sitting day for 2018. As noted previously, this included a referral of the Assistance and Access Act to this Committee for review and report by 3 April 2019 (referred to in this report as the 2019 Act Review).

2019 Act Review

1.8 The Committee announced the current review of the Assistance and Access Act and invited submissions via media release on 17 December 2018. The Committee expressed its intention to focus the 2019 Act Review on clarifying the intent of the recommendations it made in its 2018 Report and to advise the Parliament on the extent to which those recommendations as intended, were addressed.

1.9 The Committee received 71 submissions and 7 supplementary submissions (see Appendix B). The Committee did not hold public hearings as part of its review, but held classified briefings with ASIO, AFP and the Inspector-General of Intelligence and Security in February 2019.

1.10 On 12 February 2019, Mr Andrew Hastie MP (Chair), and the Hon. Mark Dreyfus QC MP (in his capacity as a member of the Committee)
made statements in the House of Representatives on behalf of the Committee to update the Parliament on the progress of the review.¹

1.11 Both advised the House that the Committee unanimously supported two further amendments to the Act to:

- bring forward the timeframe for the Independent National Security Legislation Monitor (INSLM) review of the Assistance and Access Act; and
- extend industry assistance powers provided for in the Act to Commonwealth and state anti-corruption bodies.

1.12 Mr Hastie explained that the 2018 Report included a Committee recommendation that the INSLM be required to review the Act within 18 months of its commencement. However, amendments introduced and passed on 6 December 2018 updated the Independent National Security Legislation Monitor Act 2010 to require the INSLM to commence a review of the Assistance and Access Act after it has been in force for 18 months.

Mr Hastie said the Committee felt further amendments were necessary to effect the earlier timeframe for review outlined in the 2018 Report:

The committee recommended that the commencement of the Independent National Security Legislation Monitor’s review be within 18 months of the act’s passage, to enable this expert legal advice to inform the committee’s own review of the act to commence on 13 April. It is the view of the committee that an amendment is required to clarify the time frame for the Independent National Security Legislation Monitor’s review.²

1.13 Likewise, Mr Hastie reported that the Committee desired the extension of the industry assistance powers provided for in the Act to Commonwealth and state anticorruption bodies:

The committee recognises that these commissions have a central role in ensuring integrity and accountability within public administration. They investigate, expose and prevent corruption involving or affecting public authorities and public officials... Notwithstanding the importance of these bodies, the exercise of such intrusive powers must always be oversighted. The committee is therefore of the view that the Commonwealth Ombudsman should oversight the use of these powers by state bodies. Such an extension is

¹ Both statements can be found in full via the Committee’s website.
² Mr Andrew Hastie, Chair, Parliamentary Joint Committee on Intelligence and Security, House of Representatives Hansard, Canberra, 12 February 2019, p. 76.
parallel with the Ombudsman’s oversight of the exercise of the act’s powers by state and territory police forces.³

1.14 On 13 February 2019, the Government introduced into the Senate the *Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019* to give effect to these amendments. At the time of writing, the Bill had not yet progressed beyond the Senate and a number of additional amendments had been moved.

**Committee comment**

**Matters identified by stakeholders for further consideration**

1.15 The Assistance and Access Act has attracted significant domestic and international interest since the introduction of then Bill in mid-2018 and its passage in late-2018. The Committee understands the interest as the Act introduced significant new powers on technical matters that have global implications.

1.16 The Committee takes this opportunity to thank the many submitters and witnesses that appeared at public hearings during both the 2018 Bill Review and the 2019 Act Review. Stakeholders have identified many matters for further consideration. Whilst the vast majority of this evidence focussed on Schedule 1 (industry assistance measures), stakeholders provided valuable evidence on the remaining four schedules (Schedules 2-5).

1.17 The Committee has summarised this evidence in Appendix A of this report. The Committee does not seek to respond to these matters in this report. However, noting the anticipated timing of the federal election and the upcoming statutory review by the Committee of the Assistance and Access Act⁴ to commence in April 2019, there will be opportunity for the Committee to engage with these matters in a more considered manner. The Committee is also of the view that the statutory review will be an opportunity for

---

³ Mr Andrew Hastie, Chair, Parliamentary Joint Committee on Intelligence and Security, *House of Representatives Hansard*, Canberra, 12 February 2019, p. 76.

⁴ Amendments introduced and passed by the Parliament on 6 December also expanded the scope of the review required to be undertaken by the Parliamentary Joint Committee on Intelligence and Security on the data retention regime (as set out in the *Intelligence Services Act 2001*, Part 4 section 29(1)(bc)) to include a review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. This review will commence in mid-April 2019.
industry to report on the implementation process and stakeholder engagement.

1.18 The Committee takes this opportunity to advise of its intention to examine the intersection between the Act and legislation in foreign jurisdictions, including the United States’ Clarifying Lawful Overseas Use of Data Act, in the upcoming statutory review.

Statutory review and timing of the INSLM’s review

1.19 As noted above, the Committee recommended in its 2018 Report that the INSLM be required to review the Act within 18 months of its commencement. However, Government amendments updated the Independent National Security Legislation Monitor Act 2010 to require the INSLM to commence a review of the Act after it has been in force for 18 months.

1.20 The Committee notes amendments introduced by the Government in the Senate that would align the timeframe for the INSLM’s statutory review with the Committee’s recommendation in its 2018 Report. Whilst the amendment has bipartisan support, the Committee appreciates that there may not be an opportunity for the amendment’s passage prior to the dissolution of the Parliament ahead of the upcoming federal election.

1.21 The Committee has therefore used its powers under section 7A of the Independent National Security Legislation Monitor Act 2010 to refer an inquiry to the INSLM prior to the dissolution of the Parliament. The Committee notes that this will be the first such referral by the Committee to the INSLM.

1.22 The Committee has requested the INSLM to prepare a public report on this matter, by 1 March 2020. To facilitate this significant body of work, the Committee recommends that the INSLM be provided additional resourcing.

---

5 Mr Andrew Hastie, Chair, Parliamentary Joint Committee on Intelligence and Security, House of Representatives Hansard, Canberra, 12 February 2019, p. 76; The Hon. Mr Mark Dreyfus, Member, Parliamentary Joint Committee on Intelligence and Security, House of Representatives Hansard, Canberra, 12 February 2019, p. 76.

6 Section 7A of the Independent National Security Legislation Monitor Act 2010 provides that the Committee may refer to the INSLM a matter which it becomes aware of in the course of performing its functions under subsection 29(1) of the Intelligence Services Act 2001. In referring the Assistance and Access Act to the INSLM, the Committee relies on section 29(1)(b)(ii) of the Intelligence Services Act 2001 (the TOLA Act was referred to the Committee for review and report by the Senate in a second reading amendment).
1.23 The Committee notes that a report by the INSLM, and any recommendations that the INSLM’s report might contain, will attract significant public interest and will inform the direction of the Committee’s own statutory review. The Committee is of the strong view that there must be time for public comment—and evidence provided to this Committee—on any recommendations made by the INSLM in that report. Appreciating stakeholders repeated concerns regarding sufficient timing for public comment, the timeframe for the Committee’s own statutory review must be amended. The Committee therefore recommends that section 187N of the Telecommunications (Interception and Access) Act 1979 (the legal authority for the statutory review) be amended to extend the timeframe for the Committee’s report from April 2020, to June 2020.

Recommendation 1


Recommendation 2

1.25 The Committee recommends that sufficient resources be made available to the Independent National Security Legislation Monitor to enable the review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, as referred by the Committee, and report by 1 March 2020.

Operationalisation of the Act

1.26 During the 2018 Bill Review, the Committee was advised that the evolving digital environment presents an ‘increasing challenge for law enforcement and national security agencies’ as ‘secure, encrypted communications are being used by terrorist groups and organised criminals to avoid detection and disruption’. The Committee was further advised that by 2020, it is expected that all communications of investigative value will be encrypted.

---

7 Department of Home Affairs, 2018 Bill Review Submission 18, p. 3; see also Hon Peter Dutton MP, Minister for Home Affairs, House of Representatives Hansard, 20 September 2018, p. 9671.

8 Department of Home Affairs, 2018 Bill Review Submission 18, p. 5.
The Committee has taken evidence on how the powers have been operationalised in response to identified threats, and the development of governance arrangements.\(^9\)

1.27 In the main, the Committee expects that the powers have effective safeguards and oversight, and expects that they are being used appropriately by security agencies and law enforcement.

1.28 The Committee reiterates the importance of the public assurance that is provided by effective and robust oversight measures. Democracies require intelligence agencies to be subject to independent oversight and review. Australia’s intelligence agencies have significant human and technical capabilities as well as legal powers and immunities. Without strong and credible oversight there may be a loss of trust between the agencies and the public.

1.29 The Committee wishes to encourage the Department of Home Affairs—as the agency with responsibility for national security law and policy—to work cooperatively with the Inspector-General of Intelligence and Security (which oversees the six intelligence agencies) and the Commonwealth Ombudsman (which oversees the AFP). Such cooperation, in the view of the Committee, should occur early in the development of new legislation and not once legislation has been introduced into the Parliament.

1.30 The Committee also notes the importance of adequate resourcing for both agencies, and therefore reiterates the recommendation of its 2018 Report that these agencies be properly resourced.

**Recommendation 3**

**1.31** The Committee recommends that the Government continues to ensure that the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman have sufficient resources to ensure that they can properly execute their additional responsibilities under the Assistance and Access Act.

**1.32** The Committee notes that some of the issues raised by stakeholders in the 2018 Bill Review and the 2019 Act Review are not matters to which there is consensus. Some of these matters are under current consideration by the Parliament—the Government introduced an amending Bill into the Senate

\(^9\) Australian Federal Police, *2019 Act Review Submission 21*, pp. 3-4
on 13 February 2019, to address some of those matters, and further amendments were introduced by Labor Senators addressing a wider range of matters.

1.33 Further, the INSLM’s new review of the operation, effectiveness and implementation of the amendments made by the Act will likely raise matters for public discussion. The Committee will consider the report by the INSLM on this referral in the 46th Parliament.

1.34 While noting that consideration of these matters is ongoing consideration, the Department of Home Affairs should continue to engage in robust dialogue with industry.

1.35 The Committee acknowledges the concerns raised by a range of industry and non-industry stakeholders throughout the 2018 Bill Review and the 2019 Act Review.

1.36 Some members of the Committee believe that, on balance, the Act appropriately addresses all of those concerns. Some other members of the Committee disagree with that proposition. However, all members of the Committee agree that the significant new powers introduced by the Act warrant ongoing consideration. For that reason, the Committee believes that it is appropriate that a further statutory review of the Act is scheduled to commence in April 2019.

Mr Andrew Hastie MP
Chair
April 2019
A. Summary of evidence

Matters raised by stakeholders in the 2018 Bill Review and 2019 Act Review

1.1 The Committee engaged with a broad range of stakeholders throughout its review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the 2018 Bill Review) and its review of the subsequent Act (the 2019 Act Review).

1.2 Whilst many acknowledged the challenge of new technologies, the need for properly authorised law enforcement and the need for security agencies to have access to communications; stakeholders expressed a significant number of concerns about this legislation.

1.3 This Appendix is a summary of evidence received in both the 2018 Bill Review and the 2019 Act Review. It canvasses that evidence on each of the

---

five separate schedules of the Act. As noted in the body of this Report, the Committee does not seek to respond to these matters, and their inclusion in the Appendix does not indicate whether the Committee concurs with these matters.

1.4 For clarity, the Appendix contains a brief overview of the five schedules of the amending Act, before proceeding to the matters identified by stakeholders during the 2018 Bill Review and the 2019 Act Review.

Overview of the Assistance and Access Act

1.5 The Assistance and Access Act amends a range of Commonwealth legislation in order to ‘introduce measures to better deal with the challenges posed by ubiquitous encryption’.3

1.6 The amending Act contains five schedules. Schedule 1 contains amendments to provide a series of ‘industry assistance measures’ to both lawfully request and compel industry to provide technical assistance to security agencies in response to the challenges of ubiquitous encryption.

1.7 Schedule 2 establishes powers which enable federal, state and territory law enforcement agencies to obtain covert computer access warrants when investigating certain federal offences.4

1.8 Schedules 3 and 4 amends the search warrant framework under the Crimes Act and the Customs Act to expand the ability of criminal law enforcement agencies to collect evidence from electronic devices.5

1.9 Schedule 5 clarifies that where a person voluntarily provides assistance to ASIO, that person can be conferred immunity from civil liability. It provides for new powers which enable ASIO to compel a person to provide assistance in accessing data held on a device.6

---


4 Assistance and Access Act, Explanatory Memorandum, p. 4, para. 12.

5 Assistance and Access Act, Explanatory Memorandum, p. 5, para. 15.

6 Assistance and Access Act, Explanatory Memorandum, p. 6, paras 22-23.
Schedule 1 – Industry assistance measures

1.10 The majority of submitters to the 2018 Bill Review focussed on the proposed amendments contained in Schedule 1—the industry assistance measures. Almost all expressed concerns about the amendments proposed in Schedule 1 or stated direct opposition.\(^7\)

1.11 Many of these concerns were echoed by submitters to the 2019 Act Review who felt that Government amendments passed alongside the Act did not adequately resolve these issues.8

1.12 Stakeholder issues are arranged in the following eighteen broad categories:

- **Concerns regarding security and human rights:**
  a. The potential to increase security risks as a result of industry assistance measures
  b. The impact on privacy rights and other human rights including the freedom of expression

- **Scope of potential applications:**
  c. Scope of the proposed definition of designated communications providers
  d. Scope of the assistance required to be provided (including problems with the availability of the proposed limitations)
  e. Grounds for seeking industry assistance (including concerns regarding the breadth of a relevant objective and the performance of a function or exercise of a power under law)

- **Issuing of notices and requests:**
  f. Decision-making criteria

---

g. Consultation required with the provider and compensation for costs incurred

h. Statutory time-limits for requests and notices

i. Judicial authorisation and oversight (including prior- and post-issue)

j. Centralised and efficient administration (including concerns about the breadth of agencies that may request industry assistance and recommendations for a single ‘clearing house’ and simplified contracting)

- **Enforcement and immunities:**
  k. Enforcement matters including severity of non-compliance, framing of secrecy offences

  l. Immunity provisions (including scope, extraterritorial application, users’ rights and ability to pursue civil action, and authorisation and decision-making)

- **Transparency and oversight:**
  m. Transparency (public assurance, and independent design scrutiny)

  n. Oversight of legality and propriety of administration of industry assistance

  o. Exclusion of anti-corruption commissions from Schedule 1 powers

  p. Statutory reviews and sunset periods

- **International context and alignment:**
  q. Global competitiveness

  r. Relationship with foreign laws including the United States’ *Clarifying Lawful Overseas use of Data Act*

**Industry assistance measures could increase security risks**

1.13 An overarching general concern heard by the Committee was that industry assistance measures, rather than improving security, could cause significant security risks to Australians, Australian businesses and organisations and our national security. Noting the global reach of these systems, stakeholders...
advised that systems and user’s security could be weakened across the globe.\textsuperscript{10}

1.14 It was noted by many that encryption and secure systems are critical to ensure the security of day-to-day activities and communications and are central to Australia’s national, personal and financial security.\textsuperscript{11} Indeed, end-to-end encryption has greatly improved the security of ordinary Australians against malicious actors.\textsuperscript{12} It was commented that strong encryption is the cornerstone of the modern information economy’s security and protects vast numbers of people and businesses against countless threats from petty crime to serious criminal fraud and corporate espionage.\textsuperscript{13}

1.15 Stakeholders felt that the Assistance and Access Act will erode consumers trust in secure platforms by enabling those systems to be either voluntarily or compulsorily weakened,\textsuperscript{14} with no transparency or assurance provided to

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{11} Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, p. 2; Global Digital Foundation, 2018 Bill Review Submission 21, pp. 1-2; Cisco, 2018 Bill Review Submission 42, pp. 3-4; Communications Alliance, Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association, 2018 Bill Review Submission 43, p. 3; Apple Inc, 2018 Bill Review Submission 53, p. 2; Mr Peter Young, 2019 Act Review Submission 24, p. 5.
\item \textsuperscript{12} Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, p. 6; Communications Alliance, Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association, 2018 Bill Review Submission 43, p. 3; Digital Industry Group Inc (DIGI), 2018 Bill Review Submission 78, p. 2.
\item \textsuperscript{13} Coalition of Civil Society Organisations and Technology Companies and Trade Associations, 2018 Bill Review Submission 29, p. 1; see also, Mr Nic Bresnan, 2018 Bill Review Submission 58, p. 1.
\item \textsuperscript{14} Australian Computer Society Inc, 2018 Bill Review Submission 1, p. 2, 5; Australian Industry Group, 2018 Bill Review Submission 3, p. 1; Global Digital Foundation, 2018 Bill Review Submission 21, p. 2; Mr Scott McIntyre, 2018 Bill Review Submission 24, p. 2; Australian Information Security Association, 2018 Bill Review Submission 40, p. 3; Communications Alliance, Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications
\end{itemize}
\end{footnotesize}
the public as to what systems have been impacted. In a digital age, where so much business and communication occurs through complex and interconnected systems, traditional concepts of privacy and security now equate with trust and confidence.

1.16 Stakeholders advised that the erosion of consumer trust in systems and devices could, in turn, impact the take up of automated routine system updates, presenting a challenge to the security of the entirety of those systems and impacting other users. Senetas for example, referred the Committee to advice produced by the Australian Signals Directorate which advises that one of the most critical and fundamental aspects of cybersecurity is the need to ensure that computer systems’ software is constantly kept up to date. It was identified that automated updates are necessary to ensure that vulnerabilities can be fixed quickly and efficiently, yet, in the view of stakeholders, the Act risks creating an incentive for users to disable automated update processes to preserve their trust and understanding of the software operating on their devices.

1.17 However the Department of Home Affairs asserted that the legislation ‘cannot be used to create a backdoor to encryption or impact the security of digital systems’. It argued that amendments made to the Act as it passed through Parliament ensure that ‘no requirements in the Act should be able to weaken or make vulnerable the services and devices that are used by the
1.18 Transparency and public assurance are discussed later in this Appendix.

Privacy and other human rights concerns

1.19 A large number of submitters expressed concerns regarding the Act’s impact on the right to privacy. The Australian Human Rights Commission provided a detailed submission to the 2018 Bill Review. It felt that the Assistance and Access legislation would ‘significantly limit human rights’ such as the right to privacy and that ‘it has not been demonstrated that such limitations are necessary and proportionate’. The Commission noted:

- it is difficult to confine the impact of a law that regulates different platforms used across jurisdictions to a single targeted individual. Consequently, the human rights impacts extend beyond just the people who may be of interest to law enforcement agencies and
- the ability to access the content of private communications is said to have a chilling effect on human rights as the self-adjustment of

---


behaviours by members of the community, even if their proposed actions would not have been wrongful, in the knowledge that one’s interactions and communications may be recorded and judged by unknown others.25

1.20 Other stakeholders expressed further concerns regarding the legislation’s impact on other human rights, including the right to freedom of expression.26

1.21 As a matter of law, any interference with human rights must be subject to careful and critical assessment of its necessity, legitimacy and proportionality.27 The Australian Human Rights Commission advised that the test of proportionality requires a measure to be the least intrusive instrument amongst those which might achieve the desired result.28 Serious invasions of privacy should be reserved for only the most serious incidents, and only with judicial oversight.29

1.22 Some stakeholders referred the Committee to a 2015 report by the United Nation’s Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. In that report, the Special Rapporteur advised that encryption (and the anonymity that is provided by that type of security) is essential for the enjoyment of freedom of expression and the right to privacy in the digital age.30

26 Australian Computer Society Inc, 2018 Bill Review Submission 1, p. 5; Mr Paul Wilkins, 2018 Bill Review Submission 2.1, p. 6; Ms Jan Pukallas, 2018 Bill Review Submission 15, p. 1; Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, p. 9; Mr Peter Pronczak, 2018 Bill Review Submission 25, p. 1; Mr Joe Zucco, 2018 Bill Review Submission 28, p. 1; Coalition of Civil Society Organisations and Technology Companies and Trade Associations, 2018 Bill Review Submission 29, p. 1; Access Now, 2018 Bill Review Submission 33, p. 7; Name Withheld, 2018 Bill Review Submission 68, p. 1; Name Withheld, 2018 Bill Review Submission 70, p. 1; Name Withheld, 2018 Bill Review Submission 72, p. 1; International Civil Liberties and Technology Coalition, 2019 Act Review Submission 50, p. 7.
29 For example: Australian Computer Society Inc, 2018 Bill Review Submission 1, p. 5; Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, pp. 9-10.
1.23 Stakeholders submitted a range of recommendations for the Committee’s consideration with regard to necessity, proportionality and judicial oversight. These proposals are summarised later in this Appendix.

### Scope of designated communications providers

1.24 Outside of these matters of principle, stakeholders provided much evidence on the specific detail of the Act. This included concern regarding the scope of providers that captured by the definition of a ‘designated communications provider’.  

1.25 Some noted that the definition goes beyond those ordinarily used in telecommunications services. While a number of submitters noted that it is the intent to capture the ‘global supply chain’ of communications networks, a number questioned whether it was reasonable to do so.  

---


expressed that the proposed measures will unfairly impact small businesses and startups.\textsuperscript{34}

1.26 Consequently, it was strongly recommended that both the definition of ‘designated communications provider’ and their ‘eligible activities’ be narrowed.\textsuperscript{35} More specific recommendations for amendment included:

- defining a ‘designated communications provider’ in a way that is referrable to the objective of the Act;\textsuperscript{36}
- that industry assistance measures be limited to companies with direct control and access to encrypted information;\textsuperscript{37}
- defining a ‘designated communications provider’ to apply only to those providers with a tangible and direct connection to Australia;\textsuperscript{38}
- narrow the definition to only providers of a certain size,\textsuperscript{39} or specifically, larger businesses;\textsuperscript{40}

\textsuperscript{34}Australian Computer Society Inc, 2018 Bill Review Submission 1, p. 2; Mr Joe Zucco, 2018 Bill Review Submission 28, p. 2; LaunchVic, 2018 Bill Review Submission 62, pp. 1-2; Internet Australia, 2019 Act Review Submission 29, p. 3.


\textsuperscript{36}Civil Society, 2018 Bill Review Submission 55, p. 12.

\textsuperscript{37}Law Council of Australia, 2018 Bill Review Submission 76, p. 9.


\textsuperscript{39}Internet Australia, 2018 Bill Review Submission 38, p. 12; Australian Communication Consumer Action Network, 2018 Bill Review Submission 49, p. 1.

replace definition with that already provided in the *Telecommunications Act* (sections 108-111B) to avoid confusion;\(^\text{41}\)  
remove component manufacturers from the definition;\(^\text{42}\)  
and  
defining a ‘designated communications provider’ in a manner which is limited to companies and not individual employees.\(^\text{43}\)

**Scope of assistance required**

1.27 Stakeholders expressed concern about the breadth of the types of assistance that can be requested or be compelled under industry assistance measures.\(^\text{44}\) The breadth of conduct captured is not of itself, limited to conduct that is only relevant to accessing communications, as is the stated focus of the industry assistance scheme.\(^\text{45}\)

\(^\text{41}\) Internet Australia, 2018 *Bill Review Submission 38*, p. 13.

*Telecommunications Act 1997*, subsection 110(2), defines the ‘telecommunications industry’ as follows: carriers, service providers, carriage service providers, carriage service providers who supply standard telephone services, carriage service providers who supply public mobile telecommunications services, content service providers, persons who perform cabling work (within the meaning of Division 9 of Part 21), persons who manufacture or import customer equipment or customer cabling, electronic messaging service providers, and persons who install optical fibre lines or facilities used, or for use, in or in connection with optical fibre lines.


1.28 Stakeholder concerns related to both the definition of ‘listed acts or things’ (section 317E) and ‘listed help’ for the purposes of technical capability notices (subsections 317T(4)-(6)).

1.29 For example, the Australian Human Rights Commission stated that the scope of the assistance that may be requested or compelled is ‘so vague as to potentially permit almost limitless forms of assistance’ and consequently is ‘inappropriately ambiguous and overbroad’. The Commission was of the view that such a large potential suite of assistance measures also increases the risk of agencies choosing the most rights-intrusive form of assistance as a matter of convenience, when a less restrictive measure would suffice. Professor Joseph Cannataci, the United Nations’ Special Rapporteur on the right to privacy, made similar comments.

1.30 Stakeholders recommended narrowing the definition of ‘listed acts or things’ to reduce the scope of the Act, specifically:

- removing the ability for a request or a notice to include the ‘removal of electronic protection’ from the definition of 317E,
- ensuring that the definition of ‘listed help’ is exhaustive, with any further acts or things requiring legislative amendment or legislative instrument subject to parliamentary consideration.

---

48 Professor Joseph Cannataci, United Nations’ Special Rapporteur on the right to privacy, 2018 Bill Review Submission 81, p. 9.
50 Access Now, 2018 Bill Review Submission 33, p. 15.
1.31 Other stakeholders expressed concern about the inclusion of ‘an act or thing done to conceal the fact that any thing has been done covertly’ within the definition of listed acts or things.\(^{53}\)

1.32 However, the Department of Home Affairs noted that all assistance which may be requested or compelled under the Act ‘must be related to the performance of a relevant agencies’ function conferred by, or under, a law of the Commonwealth, State or Territory’.\(^{54}\) Further, it noted that ‘the industry assistance framework is designed to support the use of existing interception powers and other lawful means of accessing content and non-content data’.\(^{55}\) It is not designed to extend the interception powers of agencies.

**Amendments introduced and passed**

1.33 The Committee sought to respond these concerns by recommending in its 2018 Report that the then Bill be amended to render the definition of ‘listed acts or things’ and ‘listed help’ which may be requested or compelled, exhaustive.\(^{56}\)

1.34 Amendments introduced and passed on 6 December 2018 partially implemented this recommendation by removing the ability for assistance, other than ‘listed acts or things’ to be compelled under technical assistance notices (TANs) (see amended subsection 317L(3)) and technical capability notices (TCNs) (see amended subsection 317T(7)).\(^{57}\)

1.35 However, amendments have not altered the ability for a technical assistance requests (TAR) to request assistance outside of those matters listed in the definition of ‘listed acts or things’ as prescribed in the Act (section 317G(6)).\(^{58}\)

---

53 Australian Computer Society Inc, 2018 Bill Review Submission 1, p. 3.
54 Department of Home Affairs, 2018 Bill Review Submission 18, p. 17.
1.36 Moreover, TCNs may also be used to compel providers to develop new capabilities in the form of ‘listed help’, a term which is not exhaustively defined under the Act. Indeed, the Act explicitly empowers the Minister for Home Affairs to proscribe additional capabilities.59

1.37 Government amendments to the Act also expanded the list of acts or things which may be the subject of a request or notice for industry assistance to include acts or things done to assist in, or to facilitate:

- giving effect to a warrant or an authorisation under a law of the Commonwealth, state or territory; and
- the effective receipt of information in connection with a warrant or authorisation under a law of the Commonwealth, state or territory.60

1.38 The Department of Home Affairs asserted that inclusion is appropriate as ‘it will only authorise activities that are immediately incidental to doing a thing that has been approved pursuant to an underlying authority subject to existing safeguards and thresholds, including judicial review’. It claimed that the amendment was necessary to ensure the powers provided by the legislation keep pace with technological advancement.61

1.39 However, in a submission to the 2019 Act Review, Internet Australia argued that the inclusion was inappropriate as it expands the scope of the legislation beyond telecommunications.62

**Problems identified with systemic weakness and systemic vulnerabilities limitation (section 317ZG)**

**Undefined or inadequate definitions**

1.40 Stakeholders who participated in the 2018 Bill Review welcomed the inclusion of a limitation aimed at preventing a TAN or a TCN from requiring the introduction of a ‘systemic weakness’ or ‘systemic vulnerability’ into a form of electronic protection.63 However, a large

---

59 Telecommunications Act, subsections 317T(4)-(6)—(Assistance and Access Act, Schedule 1, Item 8).

60 Assistance and Access Act, *Supplementary Explanatory Memorandum*, para 63.


number were concerned that the terms were not defined in the Bill and as a result, the effect of the limitation was ambiguous.  

1.41 The Committee sought to address these concerns by recommending that the Bill be amended to clarify the meaning of the terms ‘systemic weakness’ and ‘systemic vulnerability’, and to further clarify that TCNs cannot be used in this manner.

Amendments introduced and passed

1.42 Amendments introduced and passed on 6 December 2018 responded to these concerns and section 317B of the Act includes the following definitions:

**systemic vulnerability** means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.

**systemic weakness** means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.

---


66 Telecommunications Act, section 317B—(Assistance and Access Act, Schedule 1, Item 8). Emphasis added.
1.43 The term ‘target technologies’ is also defined in the Act. They are described as technology (such as a particular carriage service, electronic service, software update, equipment or device) used, by a particular person (whether directly or indirectly), regardless of whether that person can be identified.  

1.44 The terms ‘whole class of technology’ and ‘connected’ are not defined in the Act, but are described in the Supplementary Explanatory Memorandum:

   Technological classes include particular mobile device models carriage services, electronic services or software. The term is intended to encompass both old and new technology or a subclass within a broader class of technology; for example an iOS mobile operating system within a particular class, or classes, of mobile devices. Where requirements in a notice make the whole set of these items more vulnerable, it will be prohibited...

   The term ‘connected’ is intended to capture technologies associated with the particular person and reflects the modern use of communications devices and services. It is narrower than the broader notion of ‘connectivity’ with the internet.

1.45 According to the Supplementary Explanatory Memorandum, a request or notice for industry assistance does not constitute a systemic weakness or vulnerability if requirements weaken a form of electronic protection against target technologies connected to a person of interest.

1.46 The Supplementary Explanatory Memorandum suggests that the inclusion of these definitions ‘enhance[s] the protections against systemic weakness or vulnerabilities by making clear that industry assistance cannot be requested or required if it would, or would be likely, to jeopardise the security of any information held by a person other than a person connected with a target technology, including if the act or thing or requested or required would create a material risk that otherwise secure information can be accessed by an unauthorised third party’.

1.47 Likewise, the Department of Home Affairs asserted that ‘the combined effect of the new definitions and amendments… is comprehensive and ensures

---

67 Telecommunications Act, section 317B—(Assistance and Access Act, Schedule 1, Item 8). Emphasis added.

68 Assistance and Access Act, Supplementary Explanatory Memorandum, para 51-52.

69 Assistance and Access Act, Supplementary Explanatory Memorandum, para 52.

70 Assistance and Access Act, Supplementary Explanatory Memorandum, para 303.
that a solid legal guarantee to information security applies to all activities under the framework, including voluntary activities’.  

1.48 However, submitters to the 2019 Act Review were not confident that these definitions have achieved this purpose and many argued that the definitions are ambiguous or unclear.  

1.49 The Law Council of Australia asserted that ambiguity surrounding the undefined terms, ‘whole class of technology’ and ‘connected’, make it difficult to interpret the limitation on introducing systemic weakness or vulnerability. It suggested that it appears that, ‘requirements which permit the weakening of a form of electronic protection are expressly permissible [by the Act] when the electronic protection is “connected” to a person of interest’. However, the term connected is not defined in the Act and therefore ‘casts the net of technologies and their uses by individuals… very wide’. The Law Council recommended amending the Act to forbid any request or notice from requiring any act or omission that might require a provider to implement or build any weakness or vulnerability into a current or proposed product or service.  

1.50 A similar point was made by industry groups and professional associations in a joint submission. They argued that ‘the definitions are difficult to understand, ambiguous and are significantly too narrow’. They noted that the term ‘whole class of technology’ is undefined and suggested that, if its common meaning is assumed, the Act provides a too narrow definition of what constitutes a systemic weakness. Mozilla suggested that the limitation

---


73 Law Council of Australia, 2019 Act Review Submission 4, p. 30

could be strengthened by further clarifying that a ‘systemic weakness or vulnerability applies to an exploit that affects any individual product, service, or system available to more than one person’.75

1.51 Dr Chris Culnane and Associate Professor Vanessa Teague warned that the current definition may enable industry to provide technical assistance that ‘undermines the cybersecurity of millions of people, as long as something less than a “whole class of technology” is affected’.76

1.52 The Australian Human Rights Commission recommended that the Act be amended to ‘prevent assistance measures that negatively impact on the privacy or cybersecurity of a significant proportion or number of innocent third parties’.77

1.53 The Law Council, BSA | The Software Alliance and the Digital Industry Group Inc (DIGI) recommended that the limitation be recast to apply to any weakness or vulnerability, and the requirement for such conduct to amount to a systemic weakness or vulnerability, be removed.78

Exceptional access cannot avoid systemic weakness

1.54 Submissions also questioned whether access of any kind to encrypted communications can be done without introducing a systemic weakness.79 It

75 Mozilla, Submission 62, p. 7.
76 Dr Chris Culnane and Associate Professor Vanessa Teague, 2019 Act Review Submission 5, pp. 1-2.
was argued that, once developed, any such access may be capable of extension to any and all users, and could subsequently create an opening for malicious actors to take advantage of new and existing weaknesses in a system, device or platform.  

1.55 It was also identified that these broader and future opportunities are not matters required to be considered by the decision-maker when considering to issue the notice or request. While the initial development may be interpreted as not creating a systemic weakness—as it has a target of one—the ability to configure the capability to facilitate future requests would likely represent a systemic weakness or systemic vulnerability. Until the capability was destroyed after its use under the notice, its very existence ‘represents a threat to similar endpoints all over the world’.  

1.56 Similarly, Future Wise noted that without a decision-maker tracking each instance and understanding the relationship a single notice bears to all other notices issued, it is impossible to know whether the scheme overall is creating structural systemic weaknesses or vulnerabilities.
1.57  This led the Office of the Victorian Information Commissioner to conclude that the legislation will ‘create systemic risk’.  Similarly, Professor Teague and Dr Culnane advised that ‘every instance … of government-mandated weakening of cryptographic protections has eventually been shown to be exploitable by bad actors’. They further commented that ‘there is no way for a mathematical tool (whether for offence or defence) to behave differently depending on the morality of the person using it’.

1.58  It was also suggested that the legislation does not take account of how a provider would implement new capabilities required under a compulsory notice. A provider’s solution to accessing a ‘particular’ device in compliance with a one-off notice will likely neither be tied to the specific device, nor be deleted after single use.

1.59  Professor Teague and Dr Culnane suggested that the creation of a ‘backdoor’ or systemic weakness/vulnerability may not be always immediately apparent. This was echoed by the MIT Internet Policy Research Initiative.

1.60  The Office of the Australian Information Commissioner and the United Nations’ Special Rapporteur on the right to privacy advised that the risk of a single notice creating a systemic risk or systemic vulnerability presents a significant challenge to the enjoyment of privacy and other human rights by third-parties who are not the target of law enforcement or intelligence agency investigations or prosecutions.

*Limitation may not be capable of meeting its stated objective*

1.61  As a result of the concerns listed above, a number of stakeholders questioned whether the limitation on systemic weaknesses and

---

85 Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, p. 3.
86 Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, p. 3.
87 Riana Pfefferkorn, 2018 Bill Review Submission 35, pp. 5-6.
88 Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, p. 7.
90 Office of the Australian Information Commissioner, 2018 Bill Review Submission 65, p. 5; Professor Joseph Cannataci, United Nations’ Special Rapporteur on the right to privacy, 2018 Bill Review Submission 81, p. 5.
vulnerabilities was effective in meeting its stated objective.\(^{91}\) This led some to propose that TCNs be removed from the legislation completely as it was not considered possible for a new capability that would not increase the risk to other users more than it benefits law enforcement efforts.\(^{92}\)

1.62 It was also noted that while the limitation prevents agencies from requiring a provider to build a systemic weakness into their products or systems, a provider is nonetheless free to do so. Further, the legislation does not require a provider to make any effort to minimize the security impact of that systemic flaw.\(^{93}\)

**Extension of limitation to ‘listed acts or things’ other than electronic protection**

1.63 In evidence to the 2018 Bill Review, BSA | The Software Alliance noted that the systemic weakness limitation is not available to other ‘listed acts or things’ (other than the removal of a form of electronic protection). According to the Alliance, the limitation:

> …applies only to forms of electronic protection and it is unclear if, for example, the agency were to require us or our members to install software onto a device which causes it to become a listening device whether that would necessarily be prohibited by that exception.\(^{94}\)

1.64 The Law Council identified similar limitations in the proposed safeguard.\(^{95}\)

1.65 BSA | The Software Alliance was of the view that the limitation should therefore be expanded and apply to all ‘listed acts or things’.\(^{96}\)

---


\(^{94}\) Mr Darryn Lim, Director, Policy, APAC, BSA | The Software Alliance, *Proof Committee Hansard*, Canberra, 19 October 2018, p. 51.

1.66 The Committee sought to address these concerns by recommending that ‘the bill be amended to apply the ‘systemic weakness’ limitation (section 317ZG) to all ‘listed acts or things’. This recommendation was not implemented; there have been no amendments that extend the systemic weakness limitation to other types of assistance. Stakeholders remain concerned.

1.67 The Law Council suggested this issue could be resolved by replacing the term ‘electronic protection’ in subsection 317ZG(1) of the Act with the phrase ‘current or proposed product or service’.

Problems identified with the limitation relating to warrants or authorisations (section 317ZH)

1.68 The Act provides a second limitation on industry assistance measures. It prevents requests or notices from requiring a provider to engage in conduct for which a warrant or authorisation is required under certain Commonwealth and state/territory laws. An intent of this limitation, is that a request or notice does not displace the need for an agency to obtain a warrant or authorisation to view the content of that communication.

Clarifying the intent of the limitation

1.69 During the 2018 Bill Review, the Law Council was supportive of this limitation. It felt that the limitation accorded with recommendations it made during the Exposure Draft process that the legislation should expressly state that the power to request or require decryption (or an individual to facilitate opening up a password protected device) under a compulsory notice does

---

96 Mr Darryn Lim, Director, Policy, APAC, BSA | The Software Alliance, *Proof Committee Hansard*, Canberra, 19 October 2018, p. 52.


100 *Telecommunications (Interception and Access Act) 1979*; the *Surveillance Devices Act 2004*; the *Crimes Act 1914*; the *Australian Security Intelligence Organisation Act 1979*; a law of the Commonwealth (other than this Part) that is not covered by the preceding laws; and a law of a state or territory (section 317ZH(1)).
not displace the need for an agency to obtain lawful authority to view the content of a communication or electronic record.\textsuperscript{101}

1.70 However, the Law Council was concerned that the limitation is unlikely to be understood by many individuals within the diverse range of agencies that may utilise these powers and the greatly expanded range and nature of recipient entities within and outside Australia that will be subject to complex Australian law enforcement legislation for the first time. The Law Council noted that the legislation purports to apply to providers outside Australia of an electronic service that has one or more end-users in Australia, and the encrypted communication may have no other relevant link to Australia or to that of those end-users in Australia, so the provider may have little or no familiarity with Australian law.\textsuperscript{102}

1.71 Similarly, Telstra recommended that the legislation be amended to clarify that the exercise in Schedule 1 in no way provides for the content of communications to be provided to a relevant agency, and that accessing the contents of any type of communications require a warrant through established processes.\textsuperscript{103}

Amendments introduced and passed

1.72 Amendments introduced and passed on 6 December 2018 responded to these concerns by amending section 317ZH of the Bill. This section of the Act now explicitly provides that communications providers cannot be requested or required to ‘do an act or thing for which the agency, or an officer of the agency, would be required to have, or obtain, a warrant or authorisation’ under a Commonwealth, state or territory law. Unless the thing or act relates to the performance of a function or the exercise of a power already afforded to the agency under law.\textsuperscript{104}

1.73 The Law Council welcomed these amendments, but expressed some reservation about their effect by suggesting they ‘seek to add clarity to the prohibition against the side-stepping of warrants’.\textsuperscript{105} The Law Council of

\textsuperscript{101} Law Council of Australia, 2018 Bill Review Submission 76, p. 29.
\textsuperscript{102} Law Council of Australia, 2018 Bill Review Submission 76, p. 29.
\textsuperscript{103} Telstra, 2018 Bill Review Submission 44, p. 6.
\textsuperscript{104} Telecommunications Act, section 317ZH—(Assistance and Access Act, Schedule 1, Item 8).
\textsuperscript{105} Law Council of Australia, 2019 Act Review Submission 4, p. 6.
Australia also suggested that there is uncertainty regarding the potential for ASIO to issue a TAR requiring a provider to perform acts or things, including telecommunications interception, for which they would otherwise require a warrant.106

1.74  The Inspector-General of Intelligence and Security (Inspector-General) provided detailed advice on this matter during both the 2018 Bill Review and the 2019 Act Review. The Inspector-General’s advice is summarised in the following section.

Inspector-General of Intelligence and Security advice regarding warrants limitation and ‘giving effect to’ a warrant exception to the limitation

1.75  In evidence to the 2019 Act Review, the Inspector-General noted that, despite the amendments introduced and passed on 6 December 2018, the Act contains an exception to the limitation that would allow ASIO to issue a TAR, TAN or request a TCN that ‘gives effect to’ one of its warrants.107 That is, the limitation would not prevent ASIO from requesting or compelling assistance from a provider that ASIO would itself require a warrant to engage in such conduct, if such a request or notice would ‘give effect to’ a warrant otherwise obtained.108

1.76  This evidence expands upon evidence from the Inspector-General during the Committee’s 2018 Bill Review, where the Inspector-General queried that the relationship between ‘providing technical information’ (as a specific type of ‘listed act or thing’ as defined in section 317E) and ASIO’s existing questioning warrants or questioning and detention powers, and the warrants limitation.109

1.77  The Inspector-General noted advice from the Department of Home Affairs that the provision was intended to cover the doing of an act authorised under a warrant but only an extant warrant. The Inspector-General reiterated earlier suggestions that the meaning of the limitation is ambiguous and should be clarified, or, the provision simply removed and

---


107  Telecommunications Act, subsection 317ZH(4)(f)—(Assistance and Access Act, Schedule 1, Item 8).


sole reliance placed on the ‘assistance and facilitation’ exception in subsection 317ZH(4)(e).\textsuperscript{110}

1.78 In evidence to the 2019 Act Review, the Inspector-General also noted that Act potentially enables intelligence operations to utilise multiple, interrelated sources of authority (for example, TARs, TANs, TCNs and special powers warrants). It suggested that this may impede oversight activities by making it difficult to identify which powers were used in each operation without a ‘forensic search of ASIO’s records’. The Inspector-General therefore advocated for a clear requirement for ASIO to identify connections between TARs, TANs and TCNs and special powers warrants, in its reports on relevant warrants which would then form a basis for targeted searches and analysis by IGIS officials during inspections.\textsuperscript{111}

\textbf{An avenue for expanding data retention requirements}

1.79 A large number of submitters to the 2018 Bill Review questioned whether industry assistance measures could be used to expand the scope of data retention measures.\textsuperscript{112}

\textbf{Amendments introduced and passed}

1.80 The Government responded to concerns raised in the 2018 Bill Review by introducing section 317ZGA of the Act to specify that the existing data retention regime in Part 5-1A of the Telecommunications (Interception and Access) Act 1979 is the ‘explicit vehicle for expanding or contracting the data set’.\textsuperscript{113} The intent of subsection 317GA(4) is that a TCN cannot be used to require a provider to retain web browsing histories or associated metadata.\textsuperscript{114}

\begin{footnotesize}
\textsuperscript{110} Inspector-General of Intelligence and Security, 2019 Act Review Submission 1.2, pp. 7-8.

\textsuperscript{111} Inspector-General of Intelligence and Security, 2019 Act Review Submission 1.2, p. 7.


\end{footnotesize}
SUMMARY OF EVIDENCE

1.81 Evidence from the Law Council suggests it is satisfied that this amendment addressed these concerns.115

1.82 However, industry groups and professional associations made a joint submission to the 2019 Act Review which identified that without an exhaustive definition of ‘listed acts or things’ (with reference to technical assistance requests) or ‘listed help’ (with reference to technical capability notices), providers could nonetheless be requested or compelled to provide assistance could still be used to expand the scope of data retention measures, including:

- acts or things which facilitate giving effect to a warrant or authorisation, or the receipt of information in connection with a warrant or authorisation; and
- installing, maintaining, testing or using software or equipment.116

1.83 The joint submission characterised these listed acts or things as ‘loopholes’ which enable the mandatory data retention regime to be bypassed.117

Grounds for seeking industry assistance – relevant objectives

1.84 As amended, Schedule 1 establishes broad grounds or ‘relevant objectives’ on which agencies may seek industry assistance measures. The relevant objectives of TARs, TANs and TCNs differ slightly, but objectives common to all requests and notices encompass:

- the interests of Australia’s national security or safeguarding national security;
- enforcing criminal law, so far as it relates to serious Australian offences (offences with a penalty of a maximum period of three year’s imprisonment or more);118 and


118 Serious Australian offences are defined in the Assistance and Access Act as those offences with a penalty of a maximum period of three year’s imprisonment or more as a result of Australian Government amendments triggered by recommendations made in the Committee’s Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018.
assisting the enforcement of criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences.\textsuperscript{119}

1.85 Submitters to both the 2018 Bill Review and the 2019 Act Review felt that the relevant objectives are too broad and risk contravening the human rights tests of proportionality and necessity.\textsuperscript{120}

1.86 Stakeholders identified two areas for further consideration. First, stakeholders also recommended that a warrant for access to the content of communications should be made the \textit{precondition} for the issue of an industry assistance measure.\textsuperscript{121} It was argued that there is little purpose in issuing a request or notice if access to the content of the communications is not subsequently gained through a warrant or other authorisation.\textsuperscript{122} Such a requirement will ensure that a request or notice is actually relevant and give guidance as to the proportionality of the notice.\textsuperscript{123} It was also commented that the provider should also be advised that a warrant for the access to the

\textsuperscript{119} Telecommunications Act, subsections 317G(5), 317L(2) and 317T(3)—(Assistance and Access Act, Schedule 1, Item 8).


\textsuperscript{121} Mr Paul Wilkins, 2018 Bill Review Submission 2.1, p. 4; Ms Lisa Burgess, 2018 Bill Review Submission 9, p. 1; Mr Craig Marchant, 2018 Bill Review Submission 26, p. 1; Dushan Karovic-Wynne, 2018 Bill Review Submission 30, p. 2; Internet Australia, 2018 Bill Review Submission 38, p. 9; Communications Alliance, Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association, 2018 Bill Review Submission 43, p. 6; Australian Human Rights Commission, 2018 Bill Review Submission 47, p. 40.


\textsuperscript{123} Communications Alliance, Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association, 2018 Bill Review Submission 43, p. 6, 11.
content of communications has been obtained, and broadly what it permits.\textsuperscript{124}

1.87 The second matter identified in the 2018 Bill Review was that the powers should only be available in response to serious offences,\textsuperscript{125} with some proposing the use of the term as defined in \textit{Telecommunications (Interception and Access) Act 1979}.\textsuperscript{126}

1.88 In response to this second matter, the Committee sought to address concerns about the threshold for a serious offence by recommending that industry assistance measures, so far as they relate to criminal law enforcement, apply to offences with a penalty of a maximum period of three year’s imprisonment or more.\textsuperscript{127}

\textbf{Amendments introduced and passed}

\textbf{Serious offences}

1.89 Amendments introduced and passed on 6 December 2018 gave effect to the Committee’s recommendation regarding serious offences. Industry assistance measures can only be used by law enforcement agencies (Commonwealth, state or territory) where that agency is enforcing the criminal law so far as it relates to a serious offence—defined as an offence


\textsuperscript{127} Parliamentary Joint Committee on Intelligence and Security, \textit{Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018}, Recommendation 2, p. 3.
punishable by an imprisonment term of three years or more—under either Australian law or the laws of a foreign country.128

1.90 However, stakeholders in the 2019 Act Review advocated for the threshold—three years—to be raised.129

1.91 During both reviews, the Australian Human Rights Commission advocated for the definition of ‘serious offences’ in the Telecommunications Act 1997 to be aligned with the definition contained in section 5D of the Telecommunications (Interception and Access) Act 1979 (TIA Act). The TIA Act defines a serious offence as those ‘punishable by imprisonment for life or for a period, or maximum period, of at least 7 years’ which includes acts of terrorism, sabotage, espionage, foreign interference, and other serious criminal offences, including child sex offences.130

1.92 The Law Council also recommended that the definition of ‘serious offences’ be made consistent with the TIA Act so ‘serious offences’ is ‘defined as laws of the Commonwealth, a state or a territory that is punishable by a maximum term of imprisonment of seven years or more’.131

1.93 Access Now recommended removing the power to issue notices to assist the enforcement of the criminal laws of a foreign country. It was concerned that requests or notices could be issued to support law enforcement in countries with a poor human rights record, and therefore risks Australia ‘becoming the enabler of repressive and authoritarian regimes’.132

---

128 For example, technical assistance requests: see Telecommunications Act, subsection 317G(5)—(Assistance and Access Act, Schedule 1, Item 8).


Relevant objectives specific to TARs

1.94 The Government introduced other amendments, later passed by the Parliament, that clarified the relevant objective as it relates to TARs for each agency separately.

1.95 The Act explicitly notes the grounds or relevant objectives according to which each individual agency may seek the issuance of a TAR. Stakeholders expressed concerns in relation to two of the relevant objectives specific to TARs, namely:

- ASIS’s ability to issue a TAR in ‘the interests of Australia’s national security, the interests of Australia’s foreign relations or the interests of Australia’s national economic wellbeing’;\(^{133}\) and
- ASD’s ability to issue a TAR to ‘provide material, advice, and other assistance … on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means’.\(^{134}\)

1.96 In evidence to the 2018 Bill Review and the 2019 Act Review, the Australian Human Rights Commission characterised the breadth of objectives on which a TARs could be issued as ‘unjustifiably wide’. It argued that, ‘while measures that significantly limit human rights may, in some circumstances, be permissible to protect national security, it is more difficult to establish proportionality with respect to achieving comparatively less important and pressing objectives’. For example, seeking industry assistance for tax and superannuation law compliance in the interests of Australia’s national economic wellbeing.\(^{135}\)


Telecommunications Act, subsection 317G(5)(b)—(Assistance and Access Act, Schedule 1, Item 8).


Telecommunications Act, subsection 317G(5)(c)—(Assistance and Access Act, Schedule 1, Item 8).

1.97 Access Now advocated for limiting the relevant objectives for TARs. It suggested that ‘the interests of Australia’s foreign relations or the interests of Australia’s national economic well-being’ (as applicable to ASIS) should be removed and the ‘matters relating to the security and integrity of information’ (as applicable to ASD) should be modified to clarify that requests should only be issued in pursuit of improving the security and integrity of information.\(^{136}\)

*Relevant objectives specific to TANs and TCNs*

1.98 The Act does not provide agency-specific relevant objectives under which TANs or TCNS can be issued, as in the case of TARs. Rather, the Act specifies that a TAN or TCN can be issued by ASIO or a law enforcement agency for the purposes of:

- enforcing criminal law, in so far as it relates to serious Australian offences;
- assisting the enforcement of the criminal laws in force in a foreign country, in so far as those laws relate to serious foreign offences; and
- safeguarding national security.\(^{137}\)

1.99 In addition, and in respect of TANs only, ASIO or a law enforcement agency may issue a notice for a matter facilitates, or is ancillary or incidental to, a matter covered by the other three relevant objectives.\(^{138}\)

1.100 Stakeholders suggested that further consideration is required in relation to two of the relevant objectives specific to TANs and TCNs, namely:

- the performance of a function, or the exercise of a power, conferred by or under a law of the Commonwealth, a state or a territory, so far as the function or power relates to a relevant objective; and
- a matter that facilitates, or is ancillary or incidental to, a matter covered by the preceding point.

1.101 These relevant objectives do not require agencies issuing a notice to do so only in connection with their powers or their functions. Rather, the Act merely requires that requests or notices be issued in relation to a performance of a power or a function under Commonwealth or state law.


\(^{137}\) Telecommunications Act, section 317T(3)—(Assistance and Access Act, Schedule 1, Item 8).

\(^{138}\) Telecommunications Act, section 317L(2)—(Assistance and Access Act, Schedule 1, Item 8).
1.102 Stakeholders expressed some concern about the breadth of the matters for which an agency may seek to issue compulsory industry assistance measures. Some expressed further concern that a notice need only be directed towards a matter that facilitates, or is ancillary or incidental to, the performance of a power or function under law. The Law Council and Access Now recommended an amendment to remove this additional scope.

Decision-making criteria

1.103 The Act requires that requests and notices are ‘reasonable and proportionate’, ‘practicable’ and ‘technically feasible’ (sections 317P and 317V). In determining whether the requirements imposed by a requests or notices are ‘reasonable and proportionate’, the decision-maker issuing the request or notice must have regard to the following:

- the interests of national security and law enforcement;
- the legitimate interests of the designated communications provider to whom the notice relates;
- the objectives of the notice;
- the availability of other means to achieve the objectives of the notice;
- whether the industry assistance requested is in the form least intrusive on persons not of interest (for compulsory notices only);
- the legitimate expectations of the Australian community relating to privacy and cybersecurity;
- such other matters (if any) as the decision-maker considers relevant.

---


142 This decision making criteria was added as a result of Australian Government amendments triggered by Recommendation 5 of the Committee’s Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, p. 4.
1.104 The Law Council asserted that Act confers ‘an unstructured discretion to determine whether the use of the measures is “reasonable and proportionate”’.\(^{143}\) Whilst the Law Council supported the requirement that the relevant decision-maker must have regard to ‘the availability of other means to achieve the objective of the notice’, the Council expressed the following concerns:

- the proposed criteria do not provide guidance on how the individual factors are to be weighed or balanced when considering whether an industry assistance measure is reasonable and proportionate. This may mean in practice that, for example, higher weight is always given to the interests of national security and law enforcement rather than the other factors listed;
- the threshold of the individual factors are low. For example, ‘the interests of national security or law enforcement’ may capture a broad range of benign activity, and the Council recommended that a higher threshold of ‘significant’ or ‘serious national’ security and law enforcement interests be required;
- the consideration of the ‘legitimate expectations of the Australian community relating to privacy and cybersecurity’ are overly broad and vague, and should be amended to refer explicitly to the fundamental human right to privacy;
- the decision-maker should be explicitly required to consider the likely cost of complying with a request or notice, recommending that the decision-maker be required to consider ‘the legitimate interests of the designated communications provider to whom the request or notice relates, including commercial interests’, and
- the decision-making criteria be exhaustive, and that the ability for the decision-maker to consider ‘such other matters … as the case requires’ be omitted.\(^{144}\)

1.105 The Inspector-General also identified that the consideration of the ‘legitimate interests of a provider’ does not necessarily provide a clear directive to routinely consider the cumulative impact of the exercise of multiple coercive powers. Consequently, the Inspector-General suggested amendments that:

\(^{143}\) Law Council of Australia, 2018 Bill Review Submission 76, pp. 7, 21-23.

\(^{144}\) Law Council of Australia, 2018 Bill Review Submission 76, p. 22.
where a TAN is sought, a requirement for the decision-maker to assess the ‘potential for oppression arising from the exercise of multiple coercive powers against a provider’; and

- where a TAN is sought, a requirement for the requesting agency to provide information to the Attorney-General about any previous requests made and notices issued, and information about the exercise or proposed exercise of other coercive powers in relation to the provider.\(^{145}\)

1.106 Stakeholders also expressed concern about the subjective test established in the reasonable and proportionate tests.\(^{146}\) For example, Kaspersky Lab advised that a subjective state of mind of the decision-maker ‘cannot serve as a criteria for what is essentially a technical discussion, which requires specific knowledge and technical competence. This knowledge may not always be readily available in the public sector’.\(^{147}\) Kaspersky Lab noted that the subjective test presents challenges for what is otherwise a technical discussion that requires specific knowledge and technical competence.\(^{148}\) This was echoed by the Coalition of Civil Society Organisations and Technology Companies and Trade Associations, and Apple Inc.\(^{149}\)

1.107 Amendments to the decision-making criteria considered necessary by stakeholders include:

- compulsory consideration of the *necessity* of the industry assistance measure so that the availability of other means is considered prior to the request or notice being issued;\(^{150}\)

---


147 Kaspersky Lab, 2018 Bill Review Submission 13, p. 2.


• requiring agencies to have exhausted both their own means and commercially-procured means before issuing an industry assistance measure, and that these prior attempts be documented;\textsuperscript{151}

• that the benefits to the community of issuing the request or notice outweighs the costs (including the impact on trust and confidence in networked systems);\textsuperscript{152} or, similarly, whether the imperatives of law enforcement demonstrably outweigh reasonable expectations of citizens in confidentiality in communications;\textsuperscript{153}

• that human rights protections be inserted into the decision-making criteria to ensure adequate consideration and protection in all the circumstances;\textsuperscript{154}

• that the conduct required by a request or notice be the least-intrusive approach to address privacy concerns and to limit the stifling effect on innovation;\textsuperscript{155}

• that privacy protections in the decision-making criteria are bolstered, with the model in the \textit{Telecommunications (Interception and Access) Act}, section 180F proposed, where the decision-maker must consider and be satisfied on reasonable grounds that interference with privacy is justifiable and proportionate, having regard to the gravity of any conduct, the likely relevant and usefulness of the information or documents, and the reason why the disclosure or use concerned is proposed to be authorised;\textsuperscript{156}

• that consideration of the likelihood of any weakness or vulnerability that may be exploited by malicious actors;\textsuperscript{157}

\textsuperscript{151} Australian Computer Society Inc, 2018 Bill Review Submission 1, p. 3; Australian Industry Group, 2018 Bill Review Submission 3, pp. 1-3; Kaspersky Lab, 2018 Bill Review Submission 13, p. 2; Joint councils for civil liberties, 2018 Bill Review Submission 63, p. 21; Digital Industry Group Inc (DIGI), 2018 Bill Review Submission 78, p. 5.

\textsuperscript{152} Australian Industry Group, 2018 Bill Review Submission 3, p. 1.

\textsuperscript{153} Law Council of Australia, 2018 Bill Review Submission 76, pp. 7, 28-29.


\textsuperscript{156} Australian Human Rights Commission, 2018 Bill Review Submission 47, p. 29.

\textsuperscript{157} Office of the Victorian Information Commissioner, 2018 Bill Review Submission 45, p. 5; See also (with respect to conferral of immunities) Inspector-General of Intelligence and Security, 2018 Bill Review Submission 52, p. 19.
that the systemic weakness limitation in section 317ZG be specifically considered by the decision-maker,\(^\text{158}\) and

that ‘practicable’ and ‘technically feasible’ be defined.\(^\text{159}\)

1.108 In evidence to the 2018 Bill Review, the Inspector-General discussed the importance of clear decision-making criteria in legislation. The Inspector-General advised that statutory decision-making criteria ensure that the relevant matters are clearly drawn to the attention of the decision-maker in each case. Further, in the experience of the Inspector-General, a statutory requirement is the most effective way of facilitating better practice by agencies in keeping appropriately detailed and consistent record-keeping about their decisions to exercise a discretionary power. It also ensures that the relevant decision-making process is auditable, including by the Inspector-General.\(^\text{160}\)

Consultation and compensation

Consultation with a provider

1.109 The Act requires a 28-day consultation period with a provider prior to issuing a TCN (section 317W). Consultation can be waived under certain circumstances (subsection 317W(3)).

1.110 During the 2018 Bill Review, stakeholders raised a variety of concerns with respect to these consultation requirements. Broadly, these concerns included:

- that the consultation process does not adequately address residual disputes regarding technically feasibility or systemic weakness or vulnerability matters;\(^\text{161}\)

- the role and importance of a technically-competent third party to make independent evaluations was also emphasised by stakeholders;\(^\text{162}\)

---


\(^{160}\) Inspector-General of Intelligence and Security, 2018 Bill Review Submission 52, p. 17.

\(^{161}\) Kaspersky Lab, 2018 Bill Review Submission 13, pp. 1-3; Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, p. 2; Riana Pfefferkorn, 2018 Bill Review Submission 35, p. 2.

\(^{162}\) Kaspersky Lab, 2018 Bill Review Submission 13, p. 3.
that absent a definition of ‘systemic weakness’ or ‘systemic vulnerability’, it is unclear what the technical expert is attempting to detect;\textsuperscript{163}

\begin{itemize}
\item that the costs incurred by engaging a technical expert should be fully borne by government and not providers,\textsuperscript{164} and
\item that the 28-day timeframe provided for consultation is unduly short,\textsuperscript{165} and some recommended that the period be extended to 60 days.\textsuperscript{166}
\end{itemize}

\textit{Amendments introduced and passed}

1.111 These concerns led the Committee to recommend amendments to provide for an independent review mechanism by which independent legal and technical experts could assess a proposed TCN (before it has been issued) on whether:

\begin{itemize}
\item it contravenes the systemic weakness limitation;
\item the requirements it imposes are reasonable and proportionate;
\item compliance with the notice is practical and technically feasible; and
\item it is the least intrusive measure that can be used to achieve the relevant objective.\textsuperscript{167}
\end{itemize}

1.112 The Committee recommended that the findings of this assessment would be binding on the Attorney-General’s decision to issue the proposed TCN.\textsuperscript{168}

1.113 Amendments introduced and passed on 6 December 2018 provided for an independent review mechanism for proposed TCNs though the assessment will not be binding on the Attorney-General.

\textsuperscript{163} Associate Professor Vanessa Teague and Dr Chris Culnane, \textit{2018 Bill Review Submission 16}, p. 8.


\textsuperscript{166} Australian Information Industry Association, \textit{Submission 39}, p. 5.


Independent legal and technical assessment of TCNs

1.114 The Act empowers a provider, who has been issued with a TCN, to write to the Attorney-General (within the 28 day consultation period) to request that a former, senior court judge and technical expert be appointed to assess whether the proposed TCN should be issued. Together the two assessors must consider and report on whether the proposed TCN:

- contravenes the systemic weakness limitation of the Act;  
- imposes requirements which are reasonable and proportionate;  
- is practicable and technically feasible; and  
- is the least intrusive measure that would be effective in achieving the legitimate objective.

1.115 In preparing their report, the assessors must consult both the provider and the requesting agency. The assessors’ final report must be provided to the Attorney General, the provider as well as the relevant oversight agency (either the Inspector-General of Intelligence and Security or the Commonwealth Ombudsman depending on the issuing agency).

1.116 Whilst the findings of the report are not binding, the Attorney-General must have regard to it when considering the reasonableness, proportionately, practicality and technical feasibility of the proposed TCN as part of deciding to issue it.

1.117 Before the Attorney-General can approve the issuance of a TCN they must seek the approval of the Minister for Communications. This requirement was added into the legislation following a recommendation of the

---

169 Telecommunications Act, subsections 317WA(1)-(4), (13) — (Assistance and Access Act, Schedule 1, Item 8).

170 Telecommunications Act, section 317ZG — (Assistance and Access Act, Schedule 1, Item 8).

171 Telecommunications Act, subsection 317WA(7) — (Assistance and Access Act, Schedule 1, Item 8).

172 Telecommunications Act, subsection 317WA(8) — (Assistance and Access Act, Schedule 1, Item 8).

173 Telecommunications Act, subsection 317WA(6) — (Assistance and Access Act, Schedule 1, Item 8).

174 Telecommunications Act, subsection 317WA(11) — (Assistance and Access Act, Schedule 1, Item 8).
Committee.\textsuperscript{175} It was the Committee’s intention that the Minister for Communications could provide a further avenue for industry representation in relation to a proposed TCN. In deciding to authorise the TCN, the Minister for Communications must consider:

- the objectives of the notice;
- the legitimate interests of the provider;
- the impact of the notice on the efficiency and international competitiveness of the Australian telecommunications industry.\textsuperscript{176}

1.118 Whilst submitters to the 2019 Act Review welcomed the addition of a mechanism by which the appropriateness of proposed TCNs can be assessed prior to being issued, many questioned the independence of legal and technical experts appointed by an Attorney-General seeking to issue the notice.\textsuperscript{177}

1.119 Concerns were also expressed regarding the non-binding nature of the assessors’ findings\textsuperscript{178} and the fact that this review mechanism may only be sought by providers in relation to a TCN.\textsuperscript{179} For example the Australian Human Rights Commission, BSA | The Software Alliance and Access Now


\textsuperscript{176} Telecommunications Act, section 317TAAA—(Assistance and Access Act, Schedule 1, Item 8).


advocated for TARs and/or TANs to be subject to a similar review process or another appropriate form of review.\textsuperscript{180}

1.120 Evidence also highlighted the need to clarify arrangements for consultation and review in the case of urgent TANs or TCNs, the extension of an existing TCN or the issuance of a new TCN substantially similar to an earlier notice.\textsuperscript{181}

1.121 BSA | The Software Alliance noted that agencies are not required to consult providers in relation to TANs or TCNs in cases of ‘urgency’; a term undefined in the Act.\textsuperscript{182}

1.122 The Law Council noted that it appears that TCNs can only be extended with the agreement of a provider, whereas subsections 317W(7) and (8), appear to enable a substantially similar TCN to be issued to a provider without their agreement or opportunity to submit their concerns.\textsuperscript{183}

1.123 Stakeholders asserted that providers’ right to be consulted and to seek a review of a proposed TCN shouldn’t be waived in any circumstances and must inform the Attorney-General’s decision, even in cases where the consultation period is curtailed, a TCN is extended or a substantially similar TCN is issued.\textsuperscript{184}

\textit{Ongoing consultation post-issue}

1.124 A number of stakeholders noted that the legislation does not specifically enable a provider to seek review or apply for revocation of a notice.\textsuperscript{185} The Act does not include:


\textsuperscript{182} BSA | The Software Alliance, 2019 Act Review Submission 36, p. 3.

\textsuperscript{183} Law Council of Australia, 2019 Act Review Submission 4, pp. 33-34.


\textsuperscript{185} BSA | The Software Alliance, 2019 Act Review Submission 36, p. 4.
• a positive obligation on the decision-maker to consider whether the grounds for mandatory revocation are met during the period in which the notice is in force; nor
• a positive obligation on the decision-maker to consider any representations that are made by the provider about the revocation of a notice; nor
• any obligations on agency staff members to bring information to the attention of the decision-maker that suggests that the grounds of issuing have ceased to exist.\(^\text{186}\)

1.125 This led the Inspector-General to conclude that, in practice, this may limit the effectiveness of the revocation requirements.\(^\text{187}\) It suggested that the power to revoke or vary a notice be clarified beyond doubt to make compliance and oversight more effective.\(^\text{188}\)

1.126 Ms Riana Pfefferkorn, a cryptography fellow at the Stanford Law School, was of the view that such an avenue could address circumstances where implementation of the conduct required by the notice leads to widespread negative security impacts or systemic vulnerabilities.\(^\text{189}\) Similar comments were made by Optus, which further commented that a provider should have a clear avenue to seek a variation to a request or notice and be able to submit evidence which demonstrates that the practicality, reasonableness or technical viability of assistance has been adversely affected by new and changed circumstances.\(^\text{190}\)

1.127 The Australian Human Rights Commission echoed these concerns, recommending amendments that would establish a process for a provider to apply for revocation on grounds of reasonableness, proportionality, and whether a notice was practicable or technically feasible.\(^\text{191}\)

\(^{186}\) Inspector-General of Intelligence and Security, 2018 Bill Review Submission 52, p. 24.


\(^{190}\) Optus, 2018 Bill Review Submission 41, p. 8.

\(^{191}\) Australian Human Rights Commission, 2018 Bill Review Submission 47, pp. 33-34.
Extension of consultation requirements to TARs and TANs

1.128 During the 2018 Bill Review, a large number of stakeholders recommended that consultation requirements be extended to voluntary TARs and compulsory TANs. For example, the Office of the Australian Information Commissioner recommended that a technical expert assessment of all voluntary TARs and TANs should be required to confirm that the effect of the proposed conduct will not have any unintended consequences on the security of systems.

1.129 These concerns were partially addressed through amendments which inserted a new section 317PA into the Bill which require ASIO or a law enforcement agency to consult providers before issuing a TAN. This section also requires providers to be informed of their right to complain about a proposed TAN to the Inspector-General of Intelligence and Security or Commonwealth Ombudsman (depending on which agency issued the notice). However, these amendments stopped short of extending the requirement to consult to TARs.

1.130 In advocating for the extension of the requirement to consult, Optus commented that the absence of consultation creates a risk that any decision might be based on an incomplete or incorrect understanding of a service provider’s capabilities, and that such notices may not have a proper basis and may impose obligations on a provider which they cannot satisfy. In such circumstances, a provider will bear both commercial and compliance

---


194 Telecommunications Act, section 317PA—(Assistance and Access Act, Schedule 1, Item 8).

This amendment was not the subject of a Committee recommendation.

195 Telecommunications Act, subsections 317MAA(3)-(6)—(Assistance and Access Act, Schedule 1, Item 8).

risks that, in the view of Optus, is not a reasonable outcome.\textsuperscript{197} Similar comments were submitted by Telstra.\textsuperscript{198}

**Compensation for compulsory conduct**

1.131 The Act contain a ‘no profit or loss’ provision for compliance with compulsory notices unless the relevant decision-maker and the provider otherwise agree (section 317ZK), or where the Director-General of Security, the chief officer or the Attorney-General decide it is contrary to the public interest for this to occur (section 317ZK(3)). Stakeholders made recommendations for amendment to the legislation with the effect that:

- more fulsome compensation arrangements be available;\textsuperscript{199}
- a provider should have a right to compensation when it has undertaken acts as required by a notice and as a result, has suffered damage to infrastructure or loss of revenue that is directly attributable to that conduct';\textsuperscript{200} and
- provision of commercial remedies where a provider’s confidential technical information is compromised as a result of complying with a notice or request.\textsuperscript{201}

1.132 The Law Council also advised that the threshold for determining that it is not in the public interest for the ‘no profit, no loss’ provision to apply is too low. It felt that ‘there is the potential risk that it could be determined that the interests of law enforcement and national security outweigh the regulatory burden on the provider because it is in the interests of the former that its resources and funding be directed at its other efforts in law enforcement and national security’.\textsuperscript{202}

\textsuperscript{197} Optus, 2018 Bill Review Submission 41, p. 8.
\textsuperscript{198} Telstra, 2018 Bill Review Submission 44, p. 4.
\textsuperscript{199} Telstra, 2018 Bill Review Submission 44, p. 4; Australian Communication Consumer Action Network, 2018 Bill Review Submission 49, p. 2.
\textsuperscript{201} Telstra, 2018 Bill Review Submission 44, p. 3; BSA l The Software Alliance, 2018 Bill Review Submission 48, p. 2.
\textsuperscript{202} Law Council of Australia, 2019 Act Review Submission 4, p. 46.
Time limits

1.133 During the 2018 Bill Review, a range of stakeholders expressed concern regarding the absence of a strict statutory time-limit for TARs, TANs and TCNs. For example, the Office of the Victorian Information Commissioner recommended that all requests and notices should be subject to a strict time limit, commenting that it is undesirable to have open-ended vulnerabilities and that the Attorney-General should be obligated to monitor the duration, expiry and revocation of all TCNs.\(^\text{203}\)

1.134 The Committee agreed with stakeholders and recommended that the Bill be amended to provide that TANs and TCNs be subject to statutory time limits, and that any extension, renewal or variation of a TAN or TCN also be subject to a statutory time limit.\(^\text{204}\)

Amendments put and passed

1.135 Following the Committee’s recommendation, amendments were introduced and passed on 6 December 2018 which altered subsections 317MA(1A) and 317TA(1A) to ensure that TANs and TCNs cannot be in effect for longer than 12 months.\(^\text{205}\)

1.136 Amendments also introduced a measure to extend the life of a TAN or TCN past the 12 month limitation with the agreement of a provider so long as each extension does not exceed an additional 12 months.\(^\text{206}\)

1.137 However, maximum statutory time-limits were not imposed on TARs, nor recommended by the Committee in its 2018 Report. Voluntary industry assistance requests are subjected to a 90 day maximum only if an expiry date isn’t specified by the issuing agency and there is no limit on the expiry date that may be specified.\(^\text{207}\)


\(^{204}\) Parliamentary Joint Committee on Intelligence and Security, Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Recommendation 6, p. 4.


\(^{206}\) Telecommunications Act, subsections 317MA(1C)-(1D) and 317TA(1C)-(1D)—(Assistance and Access Act, Schedule 1, Item 8).

\(^{207}\) Telecommunications Act, subsection 317HA(1)—(Assistance and Access Act, Schedule 1, Item 8).
1.138 The Australian Human Rights Commission recommended a fixed time-limit for all requests and notices, commenting that a maximum duration will also help to promote more regular review by decision-makers of the necessity and appropriateness of the assistance requirements specified in them. The Law Council made similar statements, recommending amendment to:

- establish a maximum time-limit after which a TAR would have to be issued;
- include a limit on the number of fresh requests or notices that can be issued; and
- be subject to periodic review by the decision-maker;
- require providers to be informed of their right to refuse an extension of a TAR, TAN or TCN.

1.139 The Inspector-General noted that from the perspective of both legality and propriety, there are many advantages to prescribing a fixed maximum period of effect for a coercive or intrusive power, such as the power to issue a TAR. The Inspector-General therefore suggested amendments that would provide:

- a limitation on the power of the decision-maker to set an expiry date, specifically through the insertion of a statutory maximum period of effect that is aligned with the ‘default’ period of effect if no expiry date is specified; and
- an explicit limitation that a variation which extends (or further extends) the period of effect of a request or notice cannot extend the total period beyond the applicable statutory maximum. This would be consistent with existing provisions of the ASIO Act that limit powers of variation in relation to the duration of special powers warrants and authorities for the conduct of special intelligence operations;
- if no maximum period of effect is prescribed for TARs, then an express periodic review requirement should be included in the

---

Telecommunications Act or in Ministerial Guidelines to the relevant intelligence agencies.\(^{211}\)

**Judicial authorisation and oversight**

**Prior judicial authorisation**

1.140 A large number of stakeholders expressed concern that that judicial authorisation is not required before issuing a TAR, TAN or a TCN.\(^{212}\)

1.141 The Australian Human Rights Commission expressed strong concern about the appropriateness of notice-giving powers being solely afforded to decision-makers within the agencies that seek to obtain the relevant industry assistance. A self-regulating approach, according to the Commission, raises questions about effective transparency and accountability.\(^{213}\)


\(^{213}\) Australian Human Rights Commission, 2018 Bill Review Submission 47, p. 54.
1.142 A large number of submitters noted that a judicial warrant, also known as a ‘double lock’ provision, is required under the United Kingdom’s Investigatory Powers Act 2016, and recommended that a similar approach be required for Australia’s comparable scheme.  

1.143 The Investigatory Powers Act 2016 establishes similar TCN-giving powers, however that notice is subject to approval the Secretary of State in first instance, as well as a judicial commissioner of the Investigatory Powers Tribunal. The Judicial Commissioner is an independent statutory agency exercising judicial functions. In considering whether to approve the giving of a notice, the judicial commissioner must apply the same principles as would be applied by a court on an application for judicial review.

1.144 In deciding whether to approve a decision to give a relevant notice, a Judicial Commissioner must review the Secretary of State’s conclusions with regard to whether the notice is necessary and whether the conduct required by the notice is proportionate to what is sought to be achieved by that conduct. When assessing proportionality, the Judicial Commissioner must have regard to the general duties in relation to privacy that are set out in the Investigatory Powers Act.

1.145 This effectively creates a ‘double-lock warrants approval process’ whereby the Secretary of State and Judicial Commissioner must both approve the granting of certain warrants, including an interception warrant. The UK scheme also permits a provider to refer a notice back to the Secretary of State for review.

1.146 The Australian Information Industry Association noted that the UK-approach extends judicial review to questions of proportionality and

---


necessity which would enliven merits review.\textsuperscript{218} Similar comments were made in a joint submission by Communications Alliance, Australian Industry Group, Australian Information Industry Association, Australian Mobile Telecommunications Association, and in separate submissions by the Office of the Victorian Information Commissioner and the Australian Human Rights Commission.\textsuperscript{219}

1.147 Many submitters argued that any decision to issue a request or notice should made by a judicial officer and not the Attorney-General.\textsuperscript{220} The Law Council felt that this would ensure that decision-making involves someone outside the issuing agency with a ‘more objective, external perspective’. The Law Council argued that the Act’s review mechanism for TCNs does not meet this requirement as, although it involves a former senior judge, they are not the primary decision maker.\textsuperscript{221}

1.148 The Law Council supported amending the Act to require an eligible judge to refuse the issuance or variation of a TAN or TCN unless satisfied that:

- the provider can comply with the notice;
- the notice can validly be given;
- the provider has been consulted and given a reasonable opportunity to make submissions on whether the requirements to be imposed by the notice are reasonable and proportionate and whether compliance with the notice is practicable and technically feasible.\textsuperscript{222}

1.149 The Law Council noted that decision-making must be prompt and confidential on these matters. However it was of the view that judicial authorisation of industry assistance measures could be provided promptly and confidentially. In New South Wales, the Council explained, the Chief Judge of the district court rosters a judge to deal by telephone with New

\textsuperscript{218} Australian Information Industry Association, 2018 Bill Review Submission 39, p. 5.


\textsuperscript{220} Law Council of Australia, 2019 Act Review Submission 4, p. 41; Mozilla, 2019 Act Review Submission 62, p. 4; Mr Peter Young, 2019 Act Review Submission 34, p. 2; International Civil Liberties and Technology Coalition, 2019 Act Review Submission 50, pp. 4-5.

\textsuperscript{221} Law Council of Australia, 2019 Act Review Submission 4, p. 41.

\textsuperscript{222} Law Council of Australia, 2019 Act Review Submission 4, p. 42.
South Wales Police surveillance warrant requests. The process appears to function effectively and is timely.\textsuperscript{223}

1.150 Although the Council expressed strong support for external judicial authorisation, it proposed, in the alternative, that judicial review of decisions under the \textit{Administrative Decisions (Judicial Review) Act 1977} should be available, commenting that it offers applicants a simplified review process that allows courts to be more flexible in tailoring remedies for the particular circumstances of the case.\textsuperscript{224}

1.151 The Australian Human Rights Commission suggested that an external merits review, as distinct from internal merits review, would enhance the independence and quality of decision-making.\textsuperscript{225}

1.152 Strongly advocating for prior judicial authorisation, Professor Joseph Cannataci, the United Nations’ Special Rapporteur on the right to privacy, commented that ‘review needs to be undertaken by a judge who, by his or her independence from government, provides the greatest authority and legitimacy’.\textsuperscript{226} Professor Cannataci further submitted:

The limitations and safeguards revolve around the decision-maker and the Explanatory Memorandum asserts that these officers are well equipped to consider the reasonableness and proportionality of any requirements. … While ‘heart-warming’ that such a state of trust exists in Australia, greater confidence would be generated in domestic and international quarters if the legislation established an independent mechanisms that verifies proper conduct and use of these far reaching powers by such decision-makers. The role of head of an agency does not confer automatically adequate ‘oversight’ and less so when the decision-making power can be delegated, even if restricted to [senior officials].\textsuperscript{227}

Objective scrutiny independent from organisational pressures and culture is critical as the individual would necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any

\textsuperscript{223} Law Council of Australia, \textit{2018 Bill Review Submission 76}, p. 31.

\textsuperscript{224} Law Council of Australia, \textit{2018 Bill Review Submission 76}, pp. 31-32.


\textsuperscript{226} Professor Joseph Cannataci, United Nations’ Special Rapporteur on the right to privacy, \textit{2018 Bill Review Submission 81}, p. 5.

\textsuperscript{227} Professor Joseph Cannataci, United Nations’ Special Rapporteur on the right to privacy, \textit{2018 Bill Review Submission 81}, p. 6.
review proceedings, it is essential that the procedures establish and provide adequate and equivalent guarantees safeguarding his or her rights. In such circumstances, it is critical that supervisory control be provided to a judge, as judicial control offers the best guarantees of independence, impartiality, and proper procedure.  

**Ongoing oversight by the courts and grounds for appeal**

1.153 Stakeholders also advised that the legislation does not create a clear process for commencing legal proceedings in regards to industry assistance measures nor a ‘clear and meaningful’ standard for a court to apply in reviewing such a challenge. Further, it does not provide a ground for challenge by affected third parties—individuals and businesses alike. It was recommended that grounds for civil appeal should include cost, security management, risk management, business management processes, disruption to business, disparity with the Privacy Act or other common law duties, or the public interest. User’s interests are also discussed in more detail in the ‘Immunity provisions’ section of this briefing paper.

**Centralised and efficient administration**

**Single clearing house**

1.154 A number of stakeholders expressed concern about the breadth of agencies that may seek industry assistance, commenting that there should be a single ‘clearing house’ in an effort to minimise duplication or contradictory or incompatible notices being issued from multiple agencies.

---

228 Professor Joseph Cannataci, United Nations’ Special Rapporteur on the right to privacy, 2018 Bill Review Submission 81, p. 7.

229 Mr Paul Wilkins, 2018 Bill Review Submission 2.1, p. 2; Coalition of Civil Society Organisations and Technology Companies and Trade Associations, 2018 Bill Review Submission 29, pp. 5-6; Access Now, 2018 Bill Review Submission 33, p. 15; Cisco, 2018 Bill Review Submission 42, p. 5; Mozilla, 2018 Bill Review Submission 46, p. 4; International Civil Liberties and Technology Coalition, 2019 Act Review Submission 50, p. 5; Access Now, 2019 Act Review Submission 53, p. 3.


231 Mr Paul Wilkins, 2018 Bill Review Submission 2.1, p. 3.

232 Mr Paul Wilkins, 2018 Bill Review Submission 2, p. 2; Mr Paul Wilkins, 2018 Bill Review Submission 2.1, p. 2; Australian Industry Group, 2018 Bill Review Submission 3, p. 3; Optus, 2018 Bill Review
1.155 The existing Communications Access Coordinator was suggested as an appropriate body that could serve as a model for such a body.233

Amendments introduced and passed

1.156 In its 2018 Report, the Committee recommended amendments which require all TANs, issued by state and territory law enforcement, to be subjected to the approval the Australian Federal Police (AFP) Commissioner.234 This recommendation was given effect in amendments introduced and passed on 6 December 2018.

1.157 The Committee’s intent in this recommendation was to ensure that the decision to issue TANs is made consistently across jurisdictions and that duplicate, contrary or incompatible requests are not being issued by state and territory law enforcement.

1.158 However, the Department of Home Affairs raised some concerns with this requirement. In a submission to the 2019 Act Review, it claimed that requiring the AFP Commissioner to approve TANs proposed by state and territory law enforcement agencies risks:

- reducing the effectiveness of these powers for state and territory police and their willingness to use them;
- imposing an undue ‘resource and process burden’ on both the AFP and state and territory police; and
- creating ‘a structural conflict between co-equal policing agencies within the Australian federal framework’.235

Simplified contracting

1.159 Both Telstra and Optus, telecommunications carriers with existing responsibilities under the Telecommunication (Interception and Access) Act

---


1979, recommended a more efficient form of contracting, including consideration of a standard form contract.\textsuperscript{236}

1.160 In the absence of a standard contract, each provider faces the prospect of having to negotiate separate arrangements with each authorised decision-maker. Noting that there are twenty authorised agencies under the scheme, and multiple decision-makers may exist within a single agency, providers may incur significant transaction costs.\textsuperscript{237}

\textit{Voluntary assistance should be sought prior to exercise of compulsive powers}

1.161 A number of stakeholders commended the inclusion of voluntary assistance requests, commenting that it is always preferable for voluntary collaboration between government and industry rather than the exercise of compulsive powers.\textsuperscript{238} It was also noted that a collaborative and cooperative approach is more likely to result in efficient and timely outcomes.\textsuperscript{239}

1.162 It was recommended that an amendment to the legislation be sought to require a voluntary assistance request be issued before compulsive powers are used and a TAN or TCN is issued.\textsuperscript{240}

1.163 The Law Council emphasised that this graduation—mandatory prior issue of a voluntary TAR—\textit{should} be followed except where the requesting agency has reasonable cause to believe, having regard to prior dealings (which may or may not include the requesting agency) with the relevant recipient, that it will be necessary to proceed to a higher step in order to achieve a practically useful response.\textsuperscript{241}

\begin{itemize}
\item \textsuperscript{236} Optus, 2018 Bill Review Submission 41, p. 10.
\item \textsuperscript{237} Optus, 2018 Bill Review Submission 41, pp. 6-7.
\item \textsuperscript{238} Australian Industry Group, 2018 Bill Review Submission 3, p. 1; Telstra, 2018 Bill Review Submission 44, p. 4; Law Council of Australia, 2018 Bill Review Submission 76, p. 30.
\item \textsuperscript{239} Telstra, 2018 Bill Review Submission 44, p. 4.
\item \textsuperscript{241} Law Council of Australia, 2018 Bill Review Submission 76, p. 30.
\end{itemize}
BSA | The Software Alliance suggested that agencies should have to demonstrate that ‘they have exhausted all options before escalating their request to require a TAN or TCN’.  

**Enforcement matters**

**Compliance measures**

1.65 Non-compliance with a compulsory notice will attract significant civil penalties, ranging from $50,000 to $10 million. Stakeholders expressed concern about the proportionality and reasonableness of penalties for non-compliance. Furthermore, Professor Teague and Dr Culnane noted an apparent inconsistency created by the new offence for counselling circumvention of a notice (proposed section 317ZA) whilst also not limiting the ability for a provider from rectifying a systemic weakness or vulnerability. It was identified, for example, that the offence may accidentally catch providers who explain to their consumers how to keep their data secure.

1.66 Civil Society advised that the compliance provisions do not require any knowledge in relation to the existence of a compulsory notice, and, this in turn creates an opportunity for a person to unknowingly commit an offence.

1.67 Two specific recommendations were made on the compliance measures:

- that the compliance measure (section 317ZA(2)) be removed completely, and
- that a reasonable belief that a notice does not comply with the systemic weakness or systemic vulnerability limitation (section 317ZG) should be a defence to all the enforcement provisions in Division 5.

---

244 Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, pp. 6-7.
245 Civil Society, 2018 Bill Review Submission 55, p. 16.
246 Access Now, 2018 Bill Review Submission 33, p. 16.
Secrecy offences

1.168 A number of submitters to the 2018 Bill Review raised concerns regarding secrecy offences and obligations, including the scope of the offence, the severity of the proposed penalties and that an exemption for public interest disclosures should be available.248

1.169 Some questioned the reasonableness of the offences which would prohibit the disclosure of information to third parties with whom a provider may otherwise wish to consult in the assessment of technical feasibility, systemic weakness or systemic vulnerability.249

1.170 For example, BSA | The Software Alliance noted that the ‘unauthorised disclosure’ provisions in the Act do not require offenders to have intention or knowledge of wrong doing. It warned that this exposes the employees of providers to imprisonment for up to five years if they, in seeking to comply with a request or notice, innocently consult their colleagues in relation to technical questions. BSA | The Software Alliance recommended that unauthorised employee disclosures be decriminalised.250

1.171 Other concerns included that the legislation does not include provisions permitting disclosure after the facts no longer indicate that secrecy is required.251

1.172 Cisco advised that the secrecy obligations and the limited grounds for authorised disclosure could render prior statements regarding the security or lack of surveillance features to be misleading with no ability to correct that prior statement.252

---


249 Mr Joe Zucco, 2018 Bill Review Submission 28, p. 2.

250 BSA | The Software Alliance, 2019 Act review Submission 36, p. 10.

251 Coalition of Civil Society Organisations and Technology Companies and Trade Associations, 2018 Bill Review Submission 29, p. 7.

252 Cisco, 2018 Bill Review Submission 42, p. 6.
1.173 Stakeholders noted that the secrecy offences do not include a harm element.253 More specifically, concerns were expressed that the non-disclosure requirements are not limited to certain types of cases (such as where disclosure would present a threat to national security, interfere with an investigation or threaten the safety of a person).254

1.174 Stakeholders therefore recommended:

- that a harm element should be inserted into the offence;255
- that requirements be subject to strict time limits in an effort to promote government accountability about the use of industry assistance measures;256
- offences should only apply to intentional disclosures;257
- greater protections for whistle-blowers and disclosures made in the public interest258 or in accordance with the Public Interest Disclosure Act;259
- that the offence be amended to include a more comprehensive list of defences as applies with other secrecy provisions such as those in the


257 Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, p. 12.


SUMMARY OF EVIDENCE

National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018, and
- that the secrecy offence be removed altogether.

Defences available to IGIS officials

1.175 During the 2018 Bill review, the Committee also heard concerns regarding the impact of the unauthorised disclosure provisions on Inspector-General of Intelligence and Security’s ability to adduce the evidence necessary to discharge the evidential burden required by the provision. That is because current and former Inspector-General officials are under a legal disability as a result of the secrecy obligations and attendant offences in section 34 of the Inspector-General of Intelligence and Security Act 1986. To enable its oversight functions, the Inspector-General suggested an amendment to the authorised disclosure provisions to bring it into alignment with the prevailing approach to equivalent provisions under other secrecy laws, including the official secrecy offences in Division 122 of the Criminal Code as enacted by the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018.

Amendments introduced and passed

1.176 The Committee recommended that amendments be introduced to address this issue. Amendments introduced and passed on 6 December 2018 removed the evidential burden from IGIS officials in section 317ZF(5) and inserted new provisions in section 63AC into the TIA Act to enable:
- a person to make use of, or make a record of, ASIO computer access intercept information if it is in connection with the performance of IGIS officials’ powers, functions or duties;
- an IGIS official to make use of, make a record of, or tell another person about ASIO computer access intercept information if it is in connection with their powers, functions or duties; and

261 Access Now, 2018 Bill Review Submission 33, p. 16.
a person or IGIS official to make use of, make a record of, or tell another person about ASIO computer access intercept information in connection with their powers, functions or duties, even if that information was obtained by intercepting communications and the interception was for the purposes of doing a thing specified in an ASIO computer access warrant but the interception was not authorised by the ASIO computer access warrant.  

1.177 In evidence to the 2019 Act Review, the Inspector-General advised that Government amendments have ‘satisfactorily’ addressed her concerns.  

Immunity provisions  

Scope of immunity, users’ rights and limitation of civil tort  

1.178 The conferral of immunity for acts done in accordance with a TAR, TAN or a TCN is not subject to any express limitations or exclusions. Some stakeholders expressed concern about the indemnity provisions which may serve the interests of technology companies, but not those of their users.  

1.179 The Australian Human Rights Commission, for example, expressed concern that the immunities could detrimentally impact the rights of innocent third parties, including their ability to bring a civil action for loss, damage or injury cause by a provider. In such circumstances, the Commission was of the view that it is likely that a provider will opt for a more rights-intrusive option when a less restrictive measure might suffice. The Commission also noted that the immunity will remain even despite a notice being legally ineffective.  

1.180 The Commission recommended that:  

- immunities should not be available to acts that would be likely to cause significant loss or damage to third parties;  

---

264 Assistance and Access Act, Supplementary Explanatory Memorandum, paras 156-160.  
266 Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, p. 3; see also Joint councils for civil liberties, 2018 Bill Review Submission 63, p. 8.  
268 Australian Human Rights Commission, 2018 Bill Review Submission 47, p. 44.  
• criminal immunity for voluntary conduct under TARs should not be available; and
• any grant of civil or criminal immunity be reported to the relevant oversight body at time of issue.\textsuperscript{270}

1.181 Professor Teague and Dr Culnane recommended amendments that would provide redress for ordinary users harmed by a data breach that directly or indirectly is the result of an industry assistance measure.\textsuperscript{271} Similarly, the Office of the Australian Information Commissioner recommended amendments to ensure that steps taken by a provider in response to a voluntary request or compulsory notice do not enable broader misuse, interference, loss or unauthorised access, modification or disclosure of personal information.\textsuperscript{272}

1.182 Similar comments were made by the Inspector-General and Australian Information Security Association.\textsuperscript{273} For example, the Inspector-General noted that there is no specific requirement for the decision-maker to consider the potential impact on third parties who may be adversely affected by the conferral of civil immunity due to the loss of a right to a legal remedy for any loss, damage or injury caused by the providers’ actions in compliance or purported compliance with a notice.\textsuperscript{274}

\textit{Extraterritorial application and limited availability of immunities in foreign jurisdictions}

1.183 The Act provides a statutory defence for non-compliance where a provider proves that compliance would contravene a law of the foreign country (section 317ZB(5)). However, Apple expressed concern that despite the statutory defence, immunity provisions will be unavailable to actions done


\textsuperscript{271} Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, p. 9, 12.

\textsuperscript{272} Office of the Australian Information Commissioner, 2018 Bill Review Submission 65, p. 6.


pursuant in Australia in foreign jurisdictions which may enliven liability in those foreign jurisdictions. Similar concerns were expressed by Senetas.

1.184 The Law Council explained that this safe harbour provision is only available in relation to legal proceedings for imposition of a civil penalty order. That is, the safe harbour is only in respect of the imposition of a financial penalty for committing an offence, and is not a safe harbour from being found to have committed an offence. In the view of the Law Council, this creates potential reputational and financial risk and jeopardy for many organisations that are required to report as to their compliance with laws.

1.185 The Council therefore recommended that the statutory defence should not only be in respect of imposition of a financial penalty, but also a defence in relation to the offence.

Authorisation and decision-making

1.186 The authorisation requirements and statutory decision-making criteria for the provision of immunities were widely discussed in evidence to both the 2018 Bill Review and the 2019 Act Review. The Law Council expressed concern that the proposed sections conferring civil immunity on providers who comply with a voluntary request or compulsory notice are overly broad, and do not contain important safeguards on the operation of the conferral, such as exclusions or express limitations on the operation of the civil immunity.

1.187 The Law Council noted three existing avenues for the conferral of immunity in civil and criminal matters, with more robust decision-making and reporting obligations to oversight bodies including the Australian Security Intelligence Organisation Act 1979, the Intelligence Services Act 2001 and the Australian Federal Police’s controlled operations scheme. Broadly, these schemes include:

- limitations that enhance oversight of the scheme, such as reporting and notification requirements to oversight bodies and relevant ministers;
that civil and criminal immunities are only conferred with respect to acts done in proper performance of a function of the agency;

that the grant of either immunity or civil indemnification is limited for the purpose of obtaining evidence that may lead to the prosecution of a person for a serious offence;

that persons are only granted immunity or indemnification from liability if their conduct was likely to cause death, serious injury or result in the commission of a sexual offence.\(^{280}\)

1.188 The Inspector-General provided similar evidence,\(^{281}\) commenting that overseeing the conferral of immunities will be complex. It welcomed Government amendments to the legislation which require decision makers whom are deciding to issue a TAR, TAN and TCN to consider the impacts of the immunity on third parties whose rights to legal remedies against the provider may be extinguished.\(^ {282}\) However, the Inspector-General was concerned that amendments only require decision makers to consider the impacts on third parties who are not of interest to agency operations. There is no requirement to consider the impact on individuals who are of interest.

1.189 The Inspector-General questioned whether it is appropriate to limit considerations in this way ‘especially given that persons who are of interest to an intelligence agency may ultimately be eliminated as an investigative target; or may be unknowingly or unwittingly involved in prejudicial activities (for example, as a conduit through which someone else is acting)’.\(^ {283}\)

1.190 The Law Council advocated for a range of safeguards to be introduced to ensure that the conferral of immunities under the provision of industry assistance is appropriate.\(^ {284}\) Specifically, the Council recommended that the legislation be amended to provide:

\(^{280}\) Law Council of Australia, 2018 Bill Review Submission 76, pp. 24-25.


\(^{282}\) This decision making criteria was added as a result of Australian Government amendments triggered by Recommendation 5 of the Committee’s Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, p. 4.


\(^{284}\) Law Council of Australia, 2018 Bill Review Submission 76, pp. 24-25.
limitations on the conferral of civil liability for providers who provide assistance so that civil immunity is *not* conferred if the conduct results in significant loss of, or damage to, property, economic loss or physical or mental harm or injury;

- that the conferral of immunity in relation to TARs may only be provided by the Attorney-General;
- that a notice with no legal effect (by virtue of breaching the systemic weakness or systemic vulnerability limitation) will not confer criminal immunity;
- for the purpose of voluntary TARs, that criminal immunity is only conferred in relation to acts done in accordance with that request, and that the provision of civil indemnification (as opposed to criminal immunity) may be more appropriate for voluntary acts, and
- mandatory annual reporting to the Parliament on the number of times the immunities are used, the kinds of assistance requested and provided, and the extent to which the immunity provision did not apply.  

**Transparency**

**Transparency for public assurance**

1.191 Stakeholders supported provisions in the Act which provide a measure of transparency, including those provisions which:

- enable providers to publish statistics about the number of TARs, TANs or TCNs it has received in a six month block;  
- require the Minister for Home Affairs to include in their annual report, a list of the TARs, TANs and TCNs issued by interception agencies and a list of the types of serious Australian offences that industry assistance has been used to enforce during the preceding year.  

---

285 Civil indemnification may be limited to financial liability or indemnity in relation to specified conditions.


require ASIO to detail in its classified annual report the number of TARs, TANs and TCNs given to the Director-General or the Attorney-General for approval;\(^\text{289}\)

- require the Inspector-General of Intelligence and Security to be notified when a TCN consultation request is issued and to be provided with a copy of any assessors report on the proposed TCN produced.\(^\text{290}\)

1.192 However, a range of stakeholders called for greater transparency of the types of industry assistance that are being provided.\(^\text{291}\) It was argued that transparency is critical for promoting public trust in the agencies exercise of their proposed powers but also critical for retaining trust between consumers and the providers of the platforms, services and devices they use.\(^\text{292}\) These issues are addressed separately below.

**Public reporting by agencies**

1.193 It was argued by a number of stakeholders that public reporting should include:

---


\(^{290}\) Inspector-General of Intelligence and Security, 2019 Act Review Submission 1.1, p. 6.


the number of requests and notices considered, given, varied, revoked, expired and refused or challenged;
the durations of the requests and notices given;
the types of acts or things done by providers in compliance with a request or notice;
the number of requests that were refused and then compelled by way of a notice in the same or similar terms;
reasons given by a provider for not voluntarily providing the assistance;
a high-level description of the information or capability sought and the respective category of providers subject to the notice;
the number of arrests made as a consequence of assistance;
a breakdown of the types of notices issued and the types of offences for which they were connected (such as terrorism, child sex offences, organised crime etc);
the number of prosecutions for relevant offences commenced;
the expenditure of agencies in relation to requests and notices, and
whether or not information under an access warrant has been obtained and accessed by reason of exercise of industry assistance powers.293

1.194 The Australian Human Rights Commission also recommended mandatory public reporting by all agencies with powers, not just interception agencies, which would extend public reporting requirements to ASIO, ASD and ASIS.294

1.195 The Inspector-General noted that, while ASIO is subject to classified annual report requirements, these do not extend to the activities of ASD and ASIS.295

In the experience of Inspector-General, reporting requirements about the exercise by intelligence agencies of intrusive and coercive powers significantly aid independent oversight. Reporting requirements are

---


valuable as they mandate the consistent collection and maintenance of records, and the evaluation by the agency (and its Minister) of how each exercise of those powers assisted the agency to perform its functions. Reports also assist Inspector-General to:

- develop a comprehensive understanding of the way in which those powers are used;
- identify and analyse trends or patterns, including with respect to systemic issues; and
- compare the approaches of different agencies (where appropriate) including to identify best practice, or inconsistent practices not attributable to specific functions of individual agencies, or common compliance issues.

1.196 While the Inspector-General acknowledged that there may be security reasons against requiring public reporting by ASD and ASIS, it stated that it is unclear why those agencies could not at least be subject to classified reporting requirements to their Ministers and the Inspector-General in relation to their use of the scheme. The Inspector General noted that this requirement could be introduced administratively, but that ‘it has not been advised of any commitment to do so’. 296

Public disclosure by providers to consumers

1.197 Professor Teague and Dr Culnane submitted:

Ordinary users should have the opportunity to walk away based on their understanding of their risks, even if the corporation consents to the risks they are being asked to put their users’ date to. Public awareness of the extent or usage of surveillance tools is critical to allowing ordinary consumers to make appropriate risk-management decisions about the trust they place in technology. 297

1.198 Both Cisco and Apple made strong recommendations to provide for the ability to publicly disclose any form of surveillance techniques which are implemented in consumers’ devices, platforms and services. 298

---


297 Associate Professor Vanessa Teague and Dr Chris Culnane, 2018 Bill Review Submission 16, p. 3; see also Dushan Karovic-Wynne, 2018 Bill Review Submission 30, p. 1.

1.199 The Committee concurred and recommended in its 2018 Report amendments that would allow a provider to request that the Attorney-General approve disclosure of a technical capability. The recommendation made clear that the Committee expected that the Attorney-General would agree to such a request except to the extent that doing so would prejudice an investigation or compromise national security. This would complement existing provisions in the then Bill that enable a provider to disclose publically the fact that they were issued a technical capability notice.299

1.200 Amendments introduced and passed on 6 December 2018 in response to Committee recommendations partially addressed this issue.300 The Act enables providers to disclose information about a TANs or TCNs (but not about TARs) to persons within their supply chain, or where otherwise relevant, with the written permission of the relevant Government body and subject to specified conditions.301

1.201 However, the amendments to not give effect to the element of the recommendation that would establish a presumption in favour of disclosure. In a submission to the 2019 Act Review, the Department of Home Affairs indicated that, ‘the expectation that the Attorney-General would agree to such a request, and the considerations which may go to a refusal (like a compromise to national security, or revealing operation capabilities), are being set out in the administrative guidance being jointly developed with industry and agencies’.302

1.202 The International Civil Liberties and Technology Coalition welcomed the amendments, but argued that they do not adequately narrow the broad non-disclosure requirements of the Act.303


301 Assistance and Access Act, Supplementary Explanatory Memorandum, para 288-289.


303 International Civil Liberties and Technology Coalition, 2019 Act Review Submission 50, p. 6.
Transparency for independent design scrutiny

1.203 A number of stakeholders also called for greater transparency of new capabilities developed under the industry assistance scheme to facilitate independent design scrutiny. Such scrutiny is critical to ensure unintended consequences are fully appreciated and that no systemic weaknesses or vulnerabilities have been inadvertently created.

1.204 Mozilla commented that building new capabilities requires collaboration with a broad community. Capability-development that lacks independent design scrutiny risks making the product developed less secure.

1.205 The MIT Internet Policy Research Initiative advised that such transparency could be achieved in a way that avoids operational risks to law enforcement or national security investigations.

1.206 It is anticipated that some of these concerns will have been addressed by the Committee’s recommendation (and the subsequent amendments) discussed in the previous section regarding authorised public disclosure by providers for the benefit of consumer confidence.

Oversight of legality and propriety of administration of powers

1.207 A large number of stakeholders expressed the view that the Act lacks appropriate oversight of the administration of industry assistance measures once issued. It was submitted that, given the breadth of new powers, it is
‘critical that the law provide for robust oversight of authorising agencies to ensure accountability’.

In the absence of stronger controls and oversight, the benefits provided to law enforcement and intelligence agencies appeared to some stakeholders to be considerably outweighed by the risks posed to the cybersecurity of the nation.

1.208 The Uniting Church in Australia, whilst generally supportive of the proposed industry assistance measures, emphasised that broad powers must be matched by high levels of oversight and accountability to ensure that law enforcement and intelligence agencies do not misuse the powers entrusted to them.

1.209 The Office of the Victorian Information Commissioner emphasised the need for sufficient oversight from an independent body with the expertise and resources to monitor the aggregate impact of the powers. Such oversight, it was argued, could increase public confidence that the cumulative purposes to which the notices were being issued were balanced with appropriate civil liberties and human rights considerations.

1.210 Professor Joseph Cannataci, the United Nations’ Special Rapporteur on the right to privacy, noted that despite significant expansion in Australia’s national security laws in recent years, corresponding expansion in oversight is yet to be legislated.

---

Submission 54, p. 3; Name Withheld, 2018 Bill Review Submission 71, p. 3; Professor Joseph Cannataci, United Nations’ Special Rapporteur on the right to privacy, 2018 Bill Review Submission 81, p. 5.

309 Coalition of Civil Society Organisations and Technology Companies and Trade Associations, 2018 Bill Review Submission 29, p. 6; see also Office of the Victorian Information Commissioner, 2018 Bill Review Submission 45, p. 5.


311 Uniting Church in Australia, Synod of Victoria and Tasmania, 2018 Bill Review Submission 60, p. 1, 7.

312 Uniting Church in Australia, Synod of Victoria and Tasmania, 2018 Bill Review Submission 60, p. 1.


315 Professor Joseph Cannataci, United Nations’ Special Rapporteur on the right to privacy, 2018 Bill Review Submission 81, pp. 3-4.
1.211 At the federal level, the Inspector-General oversees the actions of ASIO, ASD and ASIS in making and administering industry assistance measures. The Commonwealth Ombudsman oversees the actions of the Australian Federal Police, as well as the state and territory police, in making and administering industry assistance measures.

**Amendments introduced and passed**

1.212 Following Committee recommendations, amendments were introduced and passed on 6 December 2018 which provided for the inclusion of oversight provisions which:

- require the Inspector-General of Intelligence and Security or the Commonwealth Ombudsman (depending on the issuing agency) to be notified within seven days of a TAR, TAN or a TCN being issued, varied or extended or revoked;
- require the Inspector-General of Intelligence and Security or the Commonwealth Ombudsman (depending on the issuing agency) to be notified when the relevant agency decides it would be contrary to the public interest to apply the Act’s no profit, no loss provisions;
- empower the Commonwealth Ombudsman to inspect the records of an interception agency and report their findings to the agency Chief Officer and the Minister for Home Affairs; and
- provide for the Commonwealth Ombudsman officials to receive and disclose information in connection with their oversight responsibilities.

1.213 The Department of Home Affairs asserted that these amendments will ensure that industry assistance measures are used ‘appropriately and as intended’ by strengthening ‘existing powers that authorise oversight bodies to examine the legality and propriety of the operation of the Act’.

1.214 Whilst the Commonwealth Ombudsman welcomed these new oversight powers, it was concerned about a new section 317ZRB(7) which provides for

---

the Minister for Home Affairs to delete information from Commonwealth Ombudsman reports if that information could be reasonably expected to:

- prejudice and investigation or persecution; or
- compromise any interception agency’s operational activities or methodologies.

1.215 The Commonwealth Ombudsman noted that it already provides agencies with an opportunity to advise on whether a report contains operationally sensitive material. It suggested that the power to edit reports is ‘unnecessary’ and could impact the statutory independence of the Ombudsman’s office.\(^{320}\)

1.216 The Inspector-General advised that for her oversight to be effective, it must be efficient, suggesting that record keeping and reporting by ASIO, ASD and ASIS will be critical.\(^ {321}\) The Inspector-General also suggested that oversight of the exercise of the powers would be significantly assisted by a requirement for agencies to report periodically to Inspector-General (and potentially their respective Ministers) on circumstances where:

- a provider engaged in conduct in accordance, or purported accordance, with a voluntary request or a compulsory notice;
- the provider’s conduct caused significant loss of, or serious damage to, property; or significant financial loss, or
- the provider engaged in conduct in purported compliance with the request or notice that is excluded from the immunity. (For example, as a result of the limitations in section 317ZH in relation to a notice.)\(^ {322}\)

1.217 Such a requirement would, by extension, require ASIO, ASD and ASIS to take reasonable steps to obtain visibility of the acts and things done by providers in accordance with a request or notice, as applicable. In the view of the Inspector-General, this may be implemented by including conditions in requests or notices, or associated contracts. In any event, standards of propriety in relation to the making of requests or issuing of notices would require agencies to consider the likely impact of an immunity, and to have means to ensure that the conferral and application of that immunity remain proportional.


\(^{322}\) Inspector-General of Intelligence and Security, 2018 Bill Review Submission 52, p. 30.
1.218 The Inspector-General further suggested that intelligence agencies be required to inform their Minister and the Inspector-General in relation to conduct that engages the civil and criminal immunity, where that conduct results in material loss, damage or harm to a third party, or material interference with or obstruction of the lawful use of a computer. It suggested that annual reporting of statistical information about these instances should be provided, on a classified basis if necessary.

1.219 The Inspector-General also advised that oversight of the legality and propriety of decisions made by intelligence agencies, particularly with respect to the application of the systemic weakness limitation, will be challenging. Such oversight, will require the Inspector-General to obtain, within existing resources, necessary access to independent technical expertise to inform such assessments and to critically analyse ASIO’s assessments and any information that may be provided by communications providers, and make an independent assessment.

1.220 The Law Council recommended that additional resources for oversight bodies be made available. The Committee also made a recommendation to this effect. However, it is yet to be actioned.

**Exclusion of anti-corruption commissions from Schedule 1**

1.221 In its 2018 Report, the Committee recommended that state and territory independent commissions against corruption be excluded from the scope of Schedule 1 of the Bill. For the record, it was the Committee’s intention to limit the scope of the then Bill to aid in expediting its passage in time for the Christmas and New Year break. The Government had advised the Committee that the passage of the legislation was necessary to safeguard

---

national security throughout that period. Government amendments effected this recommendation during the Bill’s passage.

1.222 A number of anti-corruption commissions have since made submissions to the 2019 Act Review highly critical of these amendments. The Commissions noted their important role in identifying and investigating misconduct, maladministration and corruption in public administration and/or in law enforcement agencies. The Law Enforcement Conduct Commission suggested that, given the expansion of law enforcement powers provided by the Assistance and Access Act, a corresponding expansion of the powers of anti-corruption commissions is required to provide appropriate oversight and to prevent abuses of these powers. The also heard that corruption is becoming more sophisticated and the use of encrypted communications is expanding. The Commissions argued that access to the industry assistance measures in Schedule 1 would better equip anti-corruption commissions to address these challenges.


1.223 The Committee has since made statements in the House of Representatives to signal its bipartisan agreement that commissions against corruption should be re-instated in Schedule 1 of the amending Act.\textsuperscript{333}

Statutory review and sunset periods

1.224 Noting the breadth of the powers provided to agencies, stakeholders proposed that the industry assistance measures be subject to a statutory review (in either two\textsuperscript{334} or three\textsuperscript{335} years).\textsuperscript{336} It was identified that such a review is an important public accountability and transparency measure.\textsuperscript{337}

1.225 Stakeholders also suggested that the amendments be subject to a sunset period.\textsuperscript{338}

1.226 The Committee also felt that further review of the Act is necessary. It recommended that the Independent National Security Legislation Monitor (INSLM) be required to review the Act within 18 months of its commencement. However, Government amendments updated the Independent National Security Legislation Monitor Act 2010 to require the INSLM to commence a review of the Act after it has been in force for 18 months.

1.227 The Committee has since made statements in the House of Representatives to signal its bipartisan agreement that this statutory review should be brought forward to accord with its original recommendation.\textsuperscript{339} Under the

\textsuperscript{333} Mr Andrew Hastie MP, Chair of the Parliamentary Joint Committee on Intelligence and Security, House of Representatives Hansard, Canberra, 12 February 2019, p. 76; the Hon. Mr Mark Dreyfus QC MP, Member, Parliamentary Joint Committee on Intelligence and Security, House of Representatives Hansard, Canberra, 12 February 2019, p. 76.

\textsuperscript{334} Law Council of Australia, 2018 Bill Review Submission 76, pp. 16-17.

\textsuperscript{335} Uniting Church in Australia, Synod of Victoria and Tasmania, 2018 Bill Review Submission 60, p. 8.

\textsuperscript{336} Future Wise, 2018 Bill Review Submission 54, p. 11; Uniting Church in Australia, Synod of Victoria and Tasmania, 2018 Bill Review Submission 60, p. 8; Office of the Australian Information Commissioner, 2018 Bill Review Submission 65, p. 10; Law Council of Australia, 2018 Bill Review Submission 76, pp. 16-17.

\textsuperscript{337} Law Council of Australia, 2018 Bill Review Submission 76, pp. 16-17.


\textsuperscript{339} Mr Andrew Hastie MP, Chair of the Parliamentary Joint Committee on Intelligence and Security, House of Representatives Hansard, Canberra, 12 February 2019, p. 76; the Hon. Mr Mark Dreyfus
Independent National Security Legislation Monitor Act 2010, the Committee has the authority to refer matters to the INSLM for inquiry and report.\textsuperscript{340}

International context and alignment

Global competitiveness

1.228 A large number of stakeholders advised that the legislation may present a ‘powerful disincentive’ for foreign investment in Australia,\textsuperscript{341} or that companies currently operating in Australia may cease to do so, both presenting a significant impact on Australia’s global competitiveness.\textsuperscript{342}

1.229 For example, Senetas advised the Committee that the legislation will damage the reputation of Australian developers and manufacturers in international markets and will result in a loss of trust and confidence in Australian cybersecurity research and development, and cybersecurity products. Senetas further warned that this will result in a decline in the current value of exports in this category and the loss of jobs and technical expertise in this industry as companies will look to relocate from Australia.\textsuperscript{343}


\textsuperscript{341} Australian Computer Society Inc, 2018 Bill Review Submission 1, p. 2; FastMail, 2019 Act Review Submission 48, p. 4.


\textsuperscript{343} Senetas, 2018 Bill Review Submission 85, pp. 1-2.
1.230 Senetas claimed that ‘Australian based providers of information technology products and services are now regularly fielding questions regarding the impact of the Act on their installed products and in the context of prospective sales engagements’. It also claimed that foreign based companies are ‘making use of the media and other material to improve their competitive position’.\(^\text{344}\)

1.231 Since the passage of the Act, and in the 2019 Act Review, the Australian Information Industry Association also advised the Committee that some of its multinational members ‘have indicated that they are considering withdrawing from the Australian market due to existing contractual and legislative compliance obligations (such as the European Union’s General Data Protection REgulation) to customers overseas’.\(^\text{345}\)

1.232 The Committee also heard from industry professionals who were concerned that the legislation would make them less hireable or jeopardise their employment, because it appears to enable individual employees to be served with a request or notice independently of their employer.\(^\text{346}\)

**Multi-jurisdictional challenges and the relationship with the CLOUD Act**

1.233 Some stakeholders questioned whether industry assistance measures would be effective in achieving the desired outcome in the context of global supply chains and existing regulations operating in foreign jurisdiction.\(^\text{347}\) This international context is highlighted when considering the number of devices, platforms and services that operate in Australia but are based overseas, particularly in the United States.

1.234 For example, the Australian Industry Group stated it was unclear to what extent the Government has taken a holistic approach and adequately considered the practicality of creating domestic laws that may be ineffective, out of step and over-reaching with other relevant jurisdiction. The Group recommended that Australia align its laws to work more effectively in

---


concert with key foreign jurisdictions and leverage international standards and best practices from other jurisdictions.  

1.235 Digital Industry Group Inc (DIGI) advised that Australia’s access to the United States’ Clarifying Lawful Overseas use of Data Act 2018, (the CLOUD Act) may be jeopardised as the legislation does not contain sufficient safeguards. DIGI is an industry group representing Facebook, Google, Instagram, Oath, Periscope, RedBubble, Twitter, Yahoo and YouTube in Australia.

1.236 The CLOUD Act expands the obligations of technology companies operating in the United States to preserve and disclose the contents of electronic communications held by those companies. It also allows the United States’ government to enter into agreements with foreign governments to enable those foreign governments to directly request assistance from American technology companies. At time of writing, the United Kingdom is the only country to progress negotiations with the United States for such an agreement, though these are yet to be finalised.

1.237 Ms Riana Pfefferkorn also advised that the Assistance and Access Act may hinder Australia’s access to the CLOUD Act. Ms Pfefferkorn provided a detailed submission to the 2018 Bill Review on the possible interaction between the two Acts, advising that:

- the CLOUD Act imposes several prerequisites on any executive agreement that may be entered into between the United States and foreign governments, including that the qualifying country (Australia) must afford ‘robust substantive and procedural protections for privacy and civil liberties’ as well as data minimisation procedures;
- any agreement entered into between Australia and the United States shall not create any obligation that providers decrypt data or otherwise prevent a provider from decrypting data;
- Australia may issue a compulsory notice in accordance with its own domestic laws, but the CLOUD Act makes clear that providers and evidence in the United States will be required to follow American law;
- the CLOUD Act requires a specific person, account, address or device be the object of the order, and as such, a compulsory notice would have to satisfy this requirement;

---

348 Australian Industry Group, 2018 Bill Review Submission 3, p. 3.
349 Digital Industry Group In (DIGI), 2018 Bill Review Submission 78, p. 4.
the CLOUD Act merely permits an American provider from disclosing user data, but that there is no guaranteed compliance;

- American law prohibits—despite a CLOUD-Act agreement—voluntary interceptions or disclosures, rendering voluntary TARs potentially ineffective, and

- an American provider may not be willing, and even unable, to comply with a compulsory notice as the range of ‘listed acts or things’ go beyond what United States’ law requires of those providers.\(^{350}\)

1.238 Ms Pfefferkorn advised that perhaps the greatest challenge presented by the legislation is that the CLOUD Act requires that an order issued by the foreign government (Australia) shall be subject to review or oversight by a court, judge, magistrate or other independent authority prior to, or in proceedings regarding, enforcement of the order.\(^{351}\) It is not clear whether the Assistance and Access Act would satisfy this threshold.

**Schedule 2 – Computer access warrants**

1.239 Schedule 2 of the Assistance and Access Act amended a number of separate acts to:

- reform existing computer access warrants in the case of ASIO,
- extend a similar warrant power to law enforcement agencies, and
- establish an avenue for foreign governments and international courts and tribunals to make requests for assistance in accessing data via a computer access warrant.

1.240 The following sections discuss these powers separately, and include a synopsis of each power and possible matters for further consideration relevant to the respective powers.

**ASIO warrants for computer access**

*Synopsis*

1.241 The Assistance and Access Act amends ASIO’s existing powers for computer access under the *Australian Security Intelligence Organisation Act 1979* (ASIO Act).

---

\(^{350}\) Ms Riana Pfefferkorn, 2018 Bill Review Submission 35.1, pp. 3-8.

1.242 The ASIO Act provides three separate avenues for accessing data held on a computer:

- a computer access warrant (issued by the Attorney-General on request from the Director-General of Security) under section 25A,
- a foreign intelligence warrant (issued by the Attorney-General on advice from the Minister of Defence or the Minister for Foreign Affairs) under section 27A, and
- an authorisation for computer access (approved by the Director-General of Security or the Attorney-General under the authority of a separately obtained identified person warrant issued by the Attorney-General), under sections 27C and 27E.

Existing provisions: Computer access warrants

1.243 On request from the Director-General of Security, the Attorney-General may issue a computer access warrant if satisfied there are reasonable grounds for believing that access by ASIO to data held in a computer\(^\text{352}\) (the target computer) will substantially assist the collection of intelligence in respect of a security matter. Prior to amendment, a computer access warrant may have authorised any of the following:

- entering a premises for the purpose of obtaining data that is relevant to the security matter;
- using the target computer, a telecommunications facility, any other electronic equipment or a data storage device to:
  - obtain access to data relevant to security that is held in the target computer at any time while the warrant is in force; and
  - add, copy, delete or alter other data (though this is limited and this action cannot materially interfere with, interrupt or obstruct a communication in transit, or the lawful use by third parties, unless it is necessary to do the things specified in the warrant);
- copying any data that appears relevant to security;
- anything reasonably necessary to conceal the fact that anything has been done under the warrant;
- any other thing reasonably incidental to any of the above; and

\(^{352}\) A ‘computer’ is defined in the ASIO Act to include all or part of one or more computers, computer systems or computer networks.
the use of force that is necessary and reasonable to do the things specified in the warrant.\textsuperscript{353}

Existing provisions: Foreign intelligence warrants

1.244 Foreign intelligence warrants are issued under section 27A of the ASIO Act, and permit ASIO to conduct intelligence collection (including computer access to obtain data) on behalf of Australia’s foreign intelligence community. On the request of the Director-General of Security, the Attorney-General may authorise a foreign intelligence warrant if satisfied, on advice from the Minister for Defence or the Minister for Foreign Affairs, that the collection is in the interests of Australia’s national security, foreign relations or national economic interests.\textsuperscript{354}

Existing provisions: Authorised computer access under an identified person warrant

1.245 Identified person warrants are issued under section 27C of the ASIO Act, and conditionally permit ASIO to use multiple special powers against a person identified in the warrant. Issued by the Attorney-General,\textsuperscript{355} an identified person warrant does not itself permit ASIO to carry out the special powers that are specified in the warrant.

1.246 Rather, it provides conditional approval for ASIO to use special powers and a separate authorisation is required to exercise each individual special powers (such as search of premises (section 27D or computer access (section 27E)). In the case of computer access, an authorisation may permit the same types of activities lawfully done under a computer access warrant discussed

\textsuperscript{353} ASIO Act, section 25A.

\textsuperscript{354} ASIO Act, section 27A.

\textsuperscript{355} The Attorney-General may issue an identified person warrant in relation to a person if satisfied that the person is engaged in, or is reasonably suspected by the Director-General of being engaged in, or likely to engage in, activities prejudicial to security, and the issuing of the warrant will or is likely to substantially assist the collection of intelligence relevant to security (ASIO Act, section 27C).

An individual person warrant may authorise the following:

(a) access to records or other things in or on premises (search of premises and persons);
(b) access to data held in computers (computer access);
(c) the use of one or more kinds of surveillance devices; and
(d) access to postal and delivery service articles.
above. These separate authorisations may be provided by the Attorney-General or the Director-General of Security.

1.247 The Assistance and Access Act does not amend the provisions relating to identified person warrants issued by the Attorney-General. Rather, the Act amended the provisions that establish the conditions for the authorisation of computer access under the identified person warrant, specifically, section 27E of the ASIO Act.

Amendments to warrants and authorisations introduced under Assistance and Access Act

1.248 The Assistance and Access Act made three key amendments to ASIO’s computer access powers:

- authorising ASIO to undertake *telecommunications interception* for the purpose of doing any thing that is specified in the warrant, including but not limited to accessing relevant data held on, or from, a computer (which would otherwise require a separate telecommunications service warrant under sections 9 or 9A of the *Telecommunications (Interception and Access) Act 1979*);\(^{356}\)

- authorising ASIO to temporarily remove a computer or other thing from premises, for the purpose of doing any thing specified in the warrant;\(^ {357}\) and

- authorising ASIO to do things that conceal access to a computer, including for up to 28 days after the warrant ceases to be in force, or as soon as reasonably practicable after the 28-day period.\(^ {358}\)

---

\(^{356}\) For computer access warrants: ASIO Act, subparagraph 25A(4)(ba)—(Assistance and Access Act, Schedule 2, Item 6).

For foreign intelligence warrants: ASIO Act, subsection 27A(3C)—(Assistance and Access Act, Schedule 2, Item 8).


\(^{357}\) For computer access warrants: ASIO Act, subparagraph 25A(4)(ac)—(Assistance and Access Act, Schedule 2, Item 5).

For foreign intelligence warrants: ASIO Act, subsection 27A(3C)—(Assistance and Access Act, Schedule 2, Item 8).


\(^{358}\) For computer access warrants: ASIO Act, subsection 25A(8)—(Assistance and Access Act, Schedule 2, Item 7).
1.249 The amending Act also reformed ASIO’s reporting requirements. Prior to the passage of the Assistance and Access Act, the Director-General of Security had obligations to report to the Attorney-General in respect of each warrant issued under ASIO’s special powers (including computer access warrants, foreign intelligence warrants, and identified person warrants), detailing the extent to which the action undertaken under the warrant has assisted ASIO in carrying out its functions. The amendments extended this reporting function include the impact of concealment of access activities.\(^{359}\)

1.250 Amendments introduced and passed on 6 December 2018 included:

- requiring that if a computer is removed from a premises, the computer must be returned within a reasonable period, or, if returning would be prejudicial to security, when the return would no longer be prejudicial to security;\(^{360}\)
- requiring that activities to conceal access must not represent a material interference with, interrupt or obstruct communications in transit or the lawful use of that computer by a third person, or cause any material loss or damage;\(^{361}\) and
- provisions clarifying ASIO’s reporting obligations with respect to concealment of access activities authorised under warrant.\(^{362}\)

For foreign intelligence warrants: ASIO Act, subsection 27A(3C)—(Assistance and Access Act, Schedule 2, Item 8).

For identified person warrants: ASIO Act, subsection 27E(6)—(Assistance and Access Act, Schedule 2, Item 12).

\(^{359}\) ASIO Act, section 34A—(Assistance and Access Act, Schedule 2, Items 13-16A.

\(^{360}\) For computer access warrants: ASIO Act, subsections 25A(4A) and (10))—(Assistance and Access Act, Schedule 2, Items 6A and 7).

For foreign intelligence warrants: ASIO Act, section 27A(3E)—(Assistance and Access Act, Schedule 2, Item 8).

For identified person warrants: ASIO Act, subsections 25E(3A) and (8)—(Assistance and Access Act, Schedule 2, Items 11A and 12).

\(^{361}\) For computer access warrants: ASIO Act, subsection 25A(9)—(Assistance and Access Act, Schedule 2, Item 7).

For foreign intelligence warrants: ASIO Act, subsection 25A(3D)—(Assistance and Access Act, Schedule 2, Item 8).

For identified person warrants: ASIO Act, subsection 27E(7)—(Assistance and Access Act, Schedule 2, Item 12).

\(^{362}\) ASIO Act, section 34A—(Assistance and Access Act, Schedule 2, Item 16A).
Possible matters for further consideration

Threshold and scope matters

1.251 As noted above, the Assistance and Access Act has extended ASIO’s computer access warrant powers to include undertaking telecommunications interception that, prior to the passage of the amending Act, would have required a separate telecommunication access warrant under the Telecommunications (Interception and Access) Act 1979.

1.252 The threshold for a telecommunication access warrant is that the Attorney-General must be satisfied that the telecommunication service is being or is likely to be used for purposes ‘prejudicial to security’. For the same type of interception under an expanded computer access warrant, the Attorney-General need only be satisfied that access to data held in a computer will substantially assist the collection of intelligence that is ‘important in relation to security’.

1.253 The Committee received evidence during the 2018 Bill Review from stakeholders concerned by the lowering of the threshold for the same type of interception activity. These concerns remain and were echoed in evidence received by the Committee in the 2019 Act Review.

1.254 Evidence received during both reviews also indicated stakeholder concerns regarding the scope of activities that may be authorised under ASIO’s extended computer access warrant. This concern extended to the following matters:

- that any data may be obtained under a revised computer access warrant, and recommendations that further amendments be introduced to restrict the warrant to obtaining access to ‘relevant data’ only, and that the removal powers be similarly restricted, and

---

363 TIA Act, sections 9 and 9A.


365 For example: Law Council of Australia, 2019 Act Review Submission 4, p. 17.


that ASIO may use force to execute a computer access warrant—representing a significant departure from equivalent warrant powers under the TIA Act—and recommendations to remove such activity from the conduct that may be authorised under the warrant.\(^{368}\)

**Reporting obligations and effective oversight**

1.255 While amendments introduced and passed on 6 December 2018 addressed some of the IGIS concerns expressed in the 2018 Bill Review with respect to reporting requirements, not all suggestions designed to improve oversight arrangements were adopted. The IGIS advised the Committee in the subsequent 2019 Act Review that the warrant reporting requirements do not oblige ASIO to specifically identify whether a computer or other thing has been removed from premises in all instances. Rather, reporting will only be required under existing provisions, if ASIO has assessed the removal to have caused material interference with the lawful use of the computer.\(^{369}\)

1.256 The absence of a reporting obligation on this matter will make it difficult for the IGIS to oversee the exercise by ASIO of the new temporary removal powers, and its decision-making about whether a temporary removal caused a material interference. Specifically, IGIS stated it will be ‘very difficult’ to determine whether a temporary removal caused material interference with the lawful use of a computer. The IGIS was of the view that this may lead to inconsistent interpretations, and therefore inconsistent reporting practices by ASIO.

1.257 The IGIS was of the view that standing inspection functions under the *Inspector-General of Intelligence and Security Act 1986*\(^{370}\) to obtain such information on a case-by-case basis would result in ‘significant inefficiency in oversight’.\(^{371}\) The IGIS clarified that ASIO warrant reports required under different provisions of the ASIO Act are used by that office as a basis for focussing inspection activities. In the absence of a reporting requirement, the IGIS would separately ask ASIO, for each and every computer access warrant, to provide information whether a computer or other thing was...

---


\(^{370}\) Inspector-General of Intelligence and Security Act 1986, section 9.

\(^{371}\) Inspector-General of Intelligence and Security, 2019 Act Review Submission 1.2, p. 11.
removed from those premises, so that IGIS could then examine those activities (including ASIO’s decision-making about whether each removal caused a material interference).\textsuperscript{372}

**Law enforcement agency warrants and orders for computer access**

**Synopsis**

1.258 Schedule 2 amends the *Surveillance Devices Act 2004* (SD Act) and provides two new powers for law enforcement agencies to obtain computer access:

- undertaking certain activities authorised under a new *computer access warrant* regime; and
- obtaining an *assistance order* to compel a person with knowledge of a computer or computer system to assist in accessing data held on that device or system.

1.259 Both are examined below.

**Computer access warrants**

1.260 Schedule 2 provides a new power for Commonwealth, state and territory law enforcement agencies investigating a federal offence punishable by a maximum of three years imprisonment or more to obtain covert computer access warrants under the *Surveillance Devices Act 2004* (SD Act). These warrants are similar to the computer access warrants already available to ASIO, as amended by the Assistance and Access Act.\textsuperscript{373}

1.261 The new warrant power is in addition to warrants for data surveillance devices, which enable the use of software to monitor inputs and outputs from certain devices.\textsuperscript{374}

1.262 Like the existing surveillance devices regime, the amending Assistance and Access Act established the framework for law enforcement agencies to obtain computer access warrants for the following investigations and operations:

- offence investigations,
- recovery orders,

---

\textsuperscript{372} Inspector-General of Intelligence and Security, 2019 *Act Review Submission 1.2*, p. 11.

\textsuperscript{373} SD Act, Part 2, Division 4—(*Assistance and Access Act, Schedule 2, Item 49*).

\textsuperscript{374} *Assistance and Access Act, Explanatory Memorandum*, p. 91, para. 448.
SUMMARY OF EVIDENCE

- mutual assistance investigations,
- integrity operations, and
- control order access.

1.263 Table 3.1 sets out the relevant threshold that applies to the computer access warrant for the above listed investigations/operations.

**Table 1.1  Thresholds for applying for computer access warrants under the Surveillance Devices Act**

<table>
<thead>
<tr>
<th>Purpose of warrant</th>
<th>Threshold for application</th>
</tr>
</thead>
</table>
| Offence investigations | Law enforcement officer\(^{375}\) suspects on reasonable grounds that:  
(a) one or more relevant offences\(^{376}\) have been, are being, are about to be, or are likely to be, committed; and  
(b) an investigation into those offences is being, will be, or is likely to be, conducted; and  
(c) access to data held in a computer (the target computer) is necessary, in the course of that investigation, for the purpose of enabling evidence to be obtained of:  
   - (i) the commission of those offences; or  
   - (ii) the identity or location of the offenders. |
| Recovery orders | A law enforcement officer may apply for the issue of a computer access warrant if:  
(a) a recovery order is in force; and  
(b) the law enforcement officer suspects on reasonable grounds that access to data held in a computer may assist in the location and safe recovery of the child to whom the recovery order relates. |
| Mutual assistance investigations | A law enforcement officer may apply for the issue of a computer access warrant if the law enforcement officer:  
(a) is authorised to do so under a mutual assistance authorisation; |

\(^{375}\) Federal and state and territory law enforcement officers are defined in section 6A of the SD Act.

\(^{376}\) Relevant offence is defined in section 6 of the SD Act and includes an offence against the law of the Commonwealth that is punishable by a maximum term of imprisonment of 3 years or more, or for life; and an offence against a law of a State that has a federal aspect and that is punishable by a maximum term of imprisonment of 3 years or more, or for life.
and
(b) suspects on reasonable grounds that access to data held in a computer is necessary, in the course of the investigation or investigative proceeding to which the authorisation relates, for the purpose of enabling evidence to be obtained of:

- (i) the commission of the offence to which the authorisation relates; or
- (ii) the identity or location of the persons suspected of committing the offence.

**Integrity operations**

A federal law enforcement officer may apply for the issue of a computer access warrant if:

(a) an integrity authority is in effect authorising an integrity operation in relation to an offence that it is suspected has been, is being or is likely to be committed by a staff member of a target agency; and

(b) the federal law enforcement officer suspects on reasonable grounds that access to data held in a computer will assist the conduct of the integrity operation by enabling evidence to be obtained relating to the integrity, location or identity of any staff member of the target agency.

**Control order access**

A law enforcement officer may apply for the issue of a computer access warrant if:

(a) a control order is in force in relation to a person; and

(b) the law enforcement officer suspects on reasonable grounds that access to data held in a computer (the target computer) to obtain information relating to the person would be likely to substantially assist in:

- (i) protecting the public from a terrorist act; or
- (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
- (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
- (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with.
1.264 A computer access warrant for one of the above listed purposes may only be issued by an eligible Judge or Administrative Appeals Tribunal member, who must be satisfied that:

- in the case of an offence investigation— that there are reasonable grounds for the suspicion founding the application for the warrant;
- in the case of a recovery order— that such an order is in force and that there are reasonable grounds for the suspicion founding the application for the warrant;
- in the case of a mutual assistance authorisation— that such an authorisation is in force and that there are reasonable grounds for the suspicion founding the application for the warrant;
- in the case of a warrant sought for the purposes of an integrity operation— that the integrity authority for the operation is in effect, and that there are reasonable grounds for the suspicions founding the application for the warrant, and
- in the case of a control order access warrant— that a control order is in force in relation to a person, and that access to data held in the relevant target computer to obtain information relating to the person would be likely to substantially assist in:
  - protecting the public from a terrorist act, or
  - preventing the provision of support for, or the facilitation of, a terrorist act, or
  - preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or
  - determining whether the control order, or any succeeding control order, has been, or is being, complied with.\textsuperscript{377}

1.265 The computer access warrant must specify the range of things that may be lawfully undertaken by law enforcement agencies, which may include:

- entering specified premises;
- entering any premises (third party premises) for the purposes of gaining entry to, or exiting, the specified premises;
- adding, copying, deleting or altering other data in the target computer,

\textsuperscript{377} SD Act, section 27C— (Assistance and Access Act, Schedule 2, Item 49).
removing a computer or other thing from premises for the purposes of doing any thing specified in the warrant, and returning the computer or other thing to the premises;

intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing specified in the warrant and if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit;

if, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is reasonable in all the circumstances to do so:
– using any other computer or a communication in transit to access the relevant data, and
– if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit;

the use of any force that is necessary and reasonable to do the things specified in the warrant; and

activities to conceal the fact that a thing as been done under a computer access warrant.\textsuperscript{378}

1.266 A computer access warrant \textit{cannot} authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

\begin{itemize}
  \item materially interfere with, interrupt or obstruct a communication in transit, or the lawful use by other persons of a computer (unless such acts are necessary to do one or more of the things specified in the warrant), or
  \item cause any other material loss or damage to other persons lawfully using a computer.\textsuperscript{379}
\end{itemize}

1.267 A number of other provisions were also included in the Assistance and Access Act to establish:

\begin{itemize}
  \item emergency authorisation for access to data held on a target computer where:
    \begin{itemize}
      \item there is a serious risk to persons or property,
      \item urgent circumstances relating to a recovery order, and
      \item risk of loss of evidence;\textsuperscript{380}
    \end{itemize}
\end{itemize}

\textsuperscript{378} SD Act, section 27E—(Assistance and Access Act, Schedule 2, Item 49).

\textsuperscript{379} SD Act, subsection 27E(5)—(Assistance and Access Act, Schedule 2, Item 49).
SUMMARY OF EVIDENCE

- extraterritorial access to data under a computer access warrant;\(^{381}\)
- information handling restrictions, including how information is to be handled in court proceedings;\(^{382}\)
- evidentiary certificates that set out facts relevant to computer access warrants) are admissible in court proceedings as prima facie evidence of the matters stated in the certificate,\(^{383}\) and
- reporting obligations to the Minister which must include, among other things, the name of any person whose data was accessed and the benefit to the investigation or operation (as applicable).\(^{384}\)

**Assistance orders**

1.268 Separately to the computer access warrant framework, law enforcement agencies may access a computer through a compulsory *assistance order*.\(^{385}\) As amended by the Assistance and Access Act, the SD Act now provides that a law enforcement officer may apply to an eligible Judge or to a nominated AAT member for an assistance order in relation to the following investigations or operations:

- offence investigations;
- recovery orders;
- mutual assistance investigations;
- integrity operations;
- control order access; and
- emergency authorisations relating to risk of loss of evidence.

1.269 An assistance order may require a specified person to provide any information or assistance that is reasonable and necessary to allow the law enforcement officer to do one or more of the following:

- access data held in a computer that is the subject of:
  - a computer access warrant, or

---

\(^{380}\) SD Act, subsections 28(1A), 30(1)-(4), 33(2), 34(1)-(4), 35(1)-(3), 35A—(Assistance and Access Act, Schedule 2, Items 50-77).

\(^{381}\) SD Act, sections 41-42, 43A-43B—(Assistance and Access Act, Schedule 2, Items 78-87).

\(^{382}\) Assistance and Access Act, Schedule 2, Items 88-97.

\(^{383}\) SD Act, section 62—(Assistance and Access Act, Schedule 2, Items 112-113).

\(^{384}\) Assistance and Access Act, Schedule 2, Items 98-111.

\(^{385}\) SD Act, section 64A—(Assistance and Access Act, Schedule 2, Item 114).
an emergency authorisation given in response to an application under subsections 28(1A), 29(1A) or 30(1A),

- copy data held in the computer to a data storage device,
- convert into documentary form or another form intelligible to a law enforcement officer:
  - data held in the computer, or
  - data held in a data storage device to which the data was copied.\textsuperscript{386}

1.270 When issuing an assistance order, the Judge or AAT member must be satisfied that there are reasonable grounds for suspecting that access to data will assist in the investigation/operation identified in the warrant application, and that a specified person:

- is the owner or lessee of the computer or device, or
- is an employee of the owner or lessee of the computer or device, or
- is a person engaged under a contract for services by the owner or lessee of the computer or device, or
- is a person who uses or has used the computer or device, or
- is a person who is or was a system administrator for the system including the computer or device, and
- has relevant knowledge of:
  - the computer or device or a computer network of which the computer or device forms or formed a part, or
  - measures applied to protect data held in the computer or device.\textsuperscript{387}

1.271 Failure to comply with an assistance order attracts a maximum imprisonment term of 10 years or 600 penalty units, or both.\textsuperscript{388}

Amendments introduced and passed on 6 December 2018

1.272 With respect to the SD Act, additional amendments introduced and passed on 6 December 2018 included:

- if a computer is removed from a premises, the computer must be returned within a reasonable period.\textsuperscript{389}

\textsuperscript{386} SD Act, section 64A—(Assistance and Access Act, Schedule 2, Item 114).

\textsuperscript{387} SD Act, subsection 64A(8)—(Assistance and Access Act, Schedule 2, Item 114).

\textsuperscript{388} SD Act, subsections 27E(2A) and (9)—(Assistance and Access Act, Schedule 2, Item 49).
• that activities to conceal access, must not represent a material interference with, interrupt or obstruct communications in transit or the lawful use of that computer by a third person, or cause any material loss or damage;  
• clarification that the computer access warrant regime does not affect parliamentary powers, privileges and immunities; 
• requirements to notify the Commonwealth Ombudsman in relation to concealment of access under a computer access warrant within 7 days of the relevant acts being undertaken, and clarifying the powers of the Ombudsman to inspect records, and 
• that the Commonwealth will be liable for loss or injury suffered by a person resulting from activities authorised under a computer access warrant under certain conditions.

Possible matters for further consideration

Privacy impact on third parties

1.273 The Law Council remains concerned that the privacy rights of third parties under the International Covenant on Civil and Political Rights will be limited under the new computer access warrant powers in the SD Act. In the 2018 Bill Review, the Law Council recommended that the provisions be amended to minimise the impact on third party privacy rights by requiring the decision-maker (an eligible Judge or AAT member) to have regard to the rights of third parties. These concerns and recommendation was repeated in the Council’s evidence in the 2019 Act Review.

Threshold and scope matters

1.274 The Law Council remains concerned that the threshold offences for obtaining a new computer access warrant to undertake telecommunications interception in the SD Act is lower than the relevant offences required under

---

392 SD Act, section 49B— (Assistance and Access Act, Schedule 2, Item 104A).
393 SD Act, subsection 55(2B) — (Assistance and Access Act, Schedule 2, Item 111A).
394 SD Act, subsection 64(2) — (Assistance and Access Act, Schedule 2, Items 113B).
395 Law Council of Australia, 2018 Bill Review Submission 76, p. 34.
the TIA Act. Under the TIA Act, a law enforcement agency may only obtain a telecommunications access warrant for the investigation of ‘serious offences’, which is defined as an offence punishable by imprisonment for at least seven years.397 The Law Council noted that the amendments to the SD Act have effectively lowered that threshold to offences carrying a 3 year imprisonment term.398 The Council made similar observations with respect to telecommunications interception where there is a control order in force in relation to another person.399

1.275 Consequently, the Law Council recommended further consideration of amendments that would apply the same thresholds to a computer access warrant that authorised telecommunications interception as currently required under the TIA Act.400

1.276 Evidence received during both reviews also indicated stakeholder concerns regarding the scope of activities that may be authorised under a new computer access warrant. These matters are broadly similar to those concerns noted above with respect to ASIO’s revised computer access warrants, and extends to the following matters:

- that any data may be obtained under a revised computer access warrant, and recommendations that further amendments be introduced to restrict the warrant to obtaining access to ‘relevant data’ only,401 and that the removal powers be similarly restricted,402 and
- that law enforcement agencies may use force to execute a computer access warrant—representing a significant departure from equivalent warrant powers under the TIA Act—and recommendations to remove

397 TIA Act, section 5D.
398 Law Council of Australia, 2018 Bill Review Submission 76, pp. 36-37.
such activity from the conduct that may be authorised under the warrant.\textsuperscript{403}

**Assistance orders**

1.277 Stakeholders in both reviews submitted concerns regarding the assistance order regime in the SD Act. Broadly, this included:

- ambiguity in the term ‘specified person’, and whether these compulsive powers would only extend to natural persons or bodies corporate,\textsuperscript{404}
- disproportionate penalties in comparison to the penalties that apply for ‘serious offences’ elsewhere that impose 2 year penalties as opposed to the 10 year penalty for failure to comply with an assistance order,\textsuperscript{405} and
- the privilege against self-incrimination and the use of information obtained under the assistance provisions.\textsuperscript{406}

**Amendments to assist foreign governments and international courts and tribunals**

**Synopsis**

1.278 The Assistance and Access Act amends the *Mutual Assistance in Criminal Matters Act 1987* to allow requests by foreign governments for assistance in relation to data held in computers.\textsuperscript{407} The amendments allow the Attorney-General to authorise an eligible law enforcement officer to apply for a computer access warrant under section 27A of the SD Act (see below) where the Attorney-General is satisfied that:

- a criminal investigation involving an offence against the law of a foreign country (that is punishable by a maximum penalty of imprisonment for three years or more, imprisonment for life or the death penalty) has commenced in the requesting country, \textit{and}


\textsuperscript{404} Law Council of Australia, 2018 Bill Review Submission 76, p. 44.

\textsuperscript{405} Law Council of Australia, 2018 Bill Review Submission 76, p. 45; Mr Daniel Hochstrasser, 2018 Bill Review Submission 61, p. 4.

\textsuperscript{406} Australian Human Rights Commission, 2018 Bill Review Submission 47, p. 77; Mr Daniel Hochstrasser, 2018 Bill Review Submission 61, pp. 2-6; Law Council of Australia, 2018 Bill Review Submission 76, p. 46.

\textsuperscript{407} MACMA, Part IIIBB—(Assistance and Access Act, Schedule 2, Items 25 and 26).
- the requesting country requests the Attorney-General to arrange for access to data held in a target computer, and
- the requesting country has given appropriate undertakings in relation to:
  - ensuring that data obtained as a result of access under the warrant will only be used for the purpose for which it is communicated to the requesting country, and
  - the destruction of a document or other thing containing data obtained as a result of access under the warrant, and
  - any other matter the Attorney-General considers appropriate.  

1.279 This mechanism is also available for requests from the International Criminal Court and the International War Crimes Tribunal for assistance in relation to data held on computers. The provisions establish the same decision-making criteria (as described above) for the Attorney-General when considering a request from either court or tribunal.

1.280 There were no relevant amendments made to these provisions on 6 December 2018 when the then Bill was passed.

Possible matters for further consideration

1.281 During the 2018 Bill Review, the Law Council expressed concern regarding the breadth of the Attorney-General’s discretion to assist foreign government requesting assistance through a computer access warrant, commenting that the discretion may create a risk, despite good intentions, that Australian assistance prior to arrest or detention may lead to the imposition of the death penalty. This concern was echoed in evidence by the Law Council in the 2019 Act Review.

1.282 On a separate matter, the Uniting Church of Australia, Synod of Victoria and Tasmania, expressed concern in the 2018 Bill Review that some foreign jurisdictions may impose a criminal penalty lower than the three year

---

408 MACMA, section 15CC—(Assistance and Access Act, Schedule 2, Item 26).


threshold despite the fact that a comparable offence in Australia carries a three year imprisonment term. The Church proposed amendments that would allow information to be provided to the foreign government where the offence in question could carry a penalty of three years in prison or more, in either the foreign jurisdiction or under Australian law.\textsuperscript{412}

**Schedules 3 and 4—Search warrants issued under the *Crimes Act 1914* and the *Customs Act 1901***

**Synopsis of Schedule 3**

1.283 Schedule 3 of the Assistance and Access Act amended the search warrant framework under the *Crimes Act 1914* (the Crimes Act) to ‘enhance the ability of criminal law enforcement agencies to collect evidence from electronic devices under warrant’.\textsuperscript{413}

1.284 Prior to the passage of the Assistance and Access Act, section 3E of the Crimes Act provided that a warrant may be issued authorising police to search either a premises or a person for the purpose of obtaining evidential material relevant to a specified offence.\textsuperscript{414} Such a warrant may be issued by either a magistrate, or a ‘justice of the peace or other person employed in a court of a State or Territory who is authorised to issue search warrants’.

1.285 The amending Assistance and Access Act expanded the types of actions that may be authorised by a search warrant to include:

- using electronic equipment to access ‘relevant data’ that is held in a computer or data storage device found in the course of a search, in order

\textsuperscript{412} Uniting Church of Australian, Synod of Victoria and Tasmania, *2018 Bill Review Submission 60*, p. 9.

\textsuperscript{413} Explanatory Memorandum, p. 5, para 15.

\textsuperscript{414} Under section 3F of the Crimes Act, such a warrant authorises the executing officer, or constable assisting, to:

(a) if the warrant was issued in relation to a premises, enter the specified premises, take fingerprints and other forensic samples, search for and seize evidential material or other seizable items, and search or frisk a person at or near the premises in order to seize evidential material or other seizable items in their possession, or

(b) if the warrant was issued in relation to a person, search the specified person and any recently used vehicle, search and seize things in the person’s possession, take fingerprints and other forensic samples, and seize other seizable items.
to determine whether the data is evidential material of a kind specified in the warrant, and

- using electronic equipment to access relevant ‘account-based data’ in relation to a person (living or deceased) who is (or was) an owner, lessee or user of a computer found in the course of a search.415

1.286 Combined, the activities that may be authorised under an expanded search warrant are broader than those detailed in Schedule 2, or contained in the Australian Security Intelligence Organisation Act 1979. However, in contrast to those powers, the Schedule 3 search warrant powers are intended to be used overtly.

1.287 Schedule 3 also authorises police to add, copy, delete or alter other data, if necessary to obtain access to the relevant data or account-based data. If it is reasonable in all the circumstances, having regard to other methods of obtaining access, police may also use any other computer or communication in transit to access the relevant data or account-based data (i.e. remote access).416

1.288 Under the amended provisions, a search warrant could not authorise police to do anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use of a computer (unless it is necessary to execute the warrant), or to cause any other material loss or damage.417

1.289 Further, the Schedule extended the time in which a computer or data storage device may be taken to another place for analysis from 14 to 30 days,418 and increased the maximum penalty from 2 years to up to 10 years for non-compliance with an assistance order requiring a person to assist police with accessing data.419

415 Crimes Act, subsections 3F(2A) and (2B)—(Assistance and Access Act, Schedule 3, Item 3).
416 Crimes Act, subsections 3F(2A) and (2B)—(Assistance and Access Act, Schedule 3, Item 3).
417 Crimes Act, subsection 35(2C)—(Assistance and Access Act, Schedule 3, Item 3).
418 Crimes Act, subsections 3K(3A) and (3D)—(Assistance and Access Act, Schedule 3, Items 4 and 6).
419 Crimes Act, subsection 3LA(5)—(Assistance and Access Act, Schedule 3, Item 9).
Amendments introduced and passed

1.290 Amendments introduced and passed on 6 December 2018 amended Schedule 3 to assert the primacy of parliamentary privileges and immunities (new section 3SA).

1.291 There were no other amendments made to Schedule 3.

Synopsis of Schedule 4

1.292 Schedule 4 of the Assistance and Access Act amended the search warrant framework under the *Customs Act 1901* (the Customs Act) to ‘enhance the ability of the Australian Border Force (ABF) to collect evidence from electronic devices under warrant in person or remotely’.\(^{420}\)

1.293 Prior to the passage of the Assistance and Access Act, section 198 of the Customs Act provided that a judicial officer may issue a warrant authorising Australian Border Force (ABF) officers to search a premises for evidential material in relation to a specified offence.\(^{421}\) A ‘judicial officer’ may be either a magistrate, or a ‘justice of the peace or other person employed in a court of a [s]tate or [t]erritory who is authorised to issue search warrants’.\(^{422}\)

1.294 The amending Assistance and Access Act expanded the types of actions that may be authorised by a warrant to include using electronic equipment to access ‘relevant data’ that is held in a computer or data storage device found in the course of a search, in order to determine whether the data is evidential material of a kind specified in the warrant.\(^{423}\)

1.295 Similarly to search warrants under the Crimes Act (Schedule 3 above), ABF officers may now be authorised under warrant to add, copy, delete or alter other data, if necessary to obtain access to the relevant data or account-based data. If it is reasonable in all the circumstances, having regard to other methods of obtaining access, officers may use any other computer or

---


\(^{421}\) Under section 199, such a warrant authorises the executing officer to enter the specified premises, take fingerprints and other forensic samples, search for and seize evidential material, and search or frisk a person at or near the premises in order to seize evidential material or other seizable items in their possession.

\(^{422}\) *Customs Act*, section 183UA.

\(^{423}\) *Customs Act*, subsection 199(4A)—(Assistance and Access Act, Schedule 4, Item 4A).
communication in transit to access the relevant data or account-based data (i.e. remote access).  

1.296 Under the amended provisions, a search warrant could not authorise officers to do anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use of a computer (unless it is necessary to execute the warrant), or to cause any other material loss or damage.  

1.297 Schedule 3 also provided ABF officers with a new power to request a search warrant in relation to a person, in order to search for a computer or data storage device and access ‘relevant data’ that is held in a computer or data storage device.  

1.298 The Assistance and Access Act also extended the time in which a computer or data storage device may be taken to another place for analysis from 72 hours to 30 days, and increased the maximum penalty from 6 months to up to 10 years imprisonment for non-compliance with an assistance order requiring a person to assist the ABF with accessing data.  

Amendments introduced and passed  

1.299 Amendments introduced and passed on 6 December 2018 amended Schedule 4 to assert the primacy of parliamentary privileges and immunities (new section 202B).  

1.300 There were no other amendments made to Schedule 4.  

424 Customs Act, subsection 199(4A)—(Assistance and Access Act, Schedule 4, Item 4A).  

425 Customs Act, subsection 199(4B)—(Assistance and Access Act, Schedule 4, Item 4A).  

426 Customs Act, sections 199(A) and 199(B)—(Assistance and Access Act, Schedule 4, Item 5).  

427 Customs Act, subsections 200(3A), 200(3B) and 200(3C)—(Assistance and Access Act, Schedule 4, Items 6, 7 and 8).  

428 Customs Act, subsections 183UA(1) and 201A(3)—(Assistance and Access Act, Schedule 4, Items 2 and 18).
Possible matters for further consideration

Search warrants are not subject to external oversight

1.301 Whilst the expanded search warrant powers are issued by an independent authority (predominantly judicial officers), the acts authorised by that warrant are not subject to oversight.

1.302 The Commonwealth Ombudsman has standing authority to investigate once a complaint is lodged, but no ‘own motion’ inspection or reporting power with respect to Schedules 3 and 4.

Assistance orders and the privilege against self-incrimination

1.303 Both schedules amended the existing assistance order provisions that would require a person to assist law enforcement agencies with accessing data. As noted above, the Assistance and Access Act extended the penalties for non-compliance with an assistance order from 6 months imprisonment (under the Customs Act) and 2 years under the Crimes Act, to up to 10 years imprisonment under both Acts.

1.304 Several stakeholders in the 2018 Bill Review discussed assistance orders under both Schedules 3 and 4, including:

- how the orders would apply to persons who are unable to provide the required assistance, and
- the interaction of the provisions with the privilege against self-incrimination.\(^{429}\)

1.305 The AHRC, for example, considered that the explanations put forward by the Government ‘do not sufficiently justify such a substantial increase in penalties’.\(^{430}\) These matters overlap significantly with the proposals for similar assistance orders found in Schedule 2 (discussed above) and Schedule 5 (discussed below).


\(^{430}\) Australian Human Rights Commission, 2018 Bill Review Submission 47, p. 75.
Impact on privacy and other human rights

1.306 Several stakeholders in the 2018 Bill Review identified the potential impact on privacy and other human rights and questioned whether the measures were reasonable and proportionate to the challenge sought to be addressed.\(^{431}\) It was recommended that search warrants issued under Schedules 3 and 4 should only authorise access to third party computers or communications where the issuing authority is satisfied that access is necessary in all the circumstances, having regard to:

- other methods of obtaining access to the data which are as likely to be as effective, and
- the human rights of the third party, including their right to privacy.\(^{432}\)

Availability of the ‘material interference’ safeguard and definition of key terms

1.307 As noted above, a search warrant authorised under Schedule 3 or 4 cannot authorise the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use of a computer (unless it is necessary to execute the warrant), or to cause any other material loss or damage.\(^{433}\)

1.308 However, stakeholders considered the effectiveness of the safeguard is limited in light of the exception—‘unless it is necessary to do one more things specified in the warrant’.\(^{434}\) It was also noted that the terms ‘material loss’ and ‘damage’ are not defined,\(^{435}\) though the Department of Home Affairs submitted that defining the terms would ‘unnecessarily narrow their application’.\(^{436}\) In the absence of definitions, the terms will take their ordinary meaning.

---


\(^{433}\) Proposed subsection 3F(2C) of the Crimes Act and proposed subsection 199B(3) of the Customs Act contain identical safeguards.

\(^{434}\) Joint civil society, 2018 Bill Review Submission 55, p. 32.

\(^{435}\) Joint civil society, 2018 Bill Review Submission 55, p. 32.

\(^{436}\) Department of Home Affairs, 2018 Bill Review Submission 18.3, p. 15.
Extension of time period of removal of a device

1.309 The extension of the time period for the removal of a device for up to 30 days was also discussed in evidence to the 2018 Bill Review. Stakeholders commented that it would be undesirable if the extension of time simply meant that an electronic device was held in custody, but not actively used because the law enforcement agency knows it has an extended period of time.\(^{437}\) It was identified that a law enforcement agency who has obtained a search warrant under Schedule 3 or 4 should make all reasonable endeavours to examine the device in the shortest possible time.\(^{438}\)

Notification of the person subject to the search warrant

1.310 Unlike the ‘covert’ computer access warrant powers provided for in Schedule 2 to the Act, the search warrant powers amended by Schedules 3 and 4 are considered ‘overt’.\(^{439}\) The expanded search warrant powers could only be considered ‘overt’ where the person the subject of the warrant was made aware of its issue and execution.

1.311 A copy of the search warrants obtained under Schedule 3 and 4 must be provided to the person the subject of the warrant if they are present. Noting that a search warrant would enable a device to be searched remotely—and therefore, potentially, without the need for a physical presence of officers at the premises—it is possible that a person might never be made aware of the execution of a search warrant. A similar circumstance might occur if a person was not at the premises where warrant is executed by officers physically present.

Schedule 5 – ASIO device access and immunities

1.312 Schedule 5 of the Assistance and Access Act amends the Australian Security Intelligence Organisation Act 1979 (ASIO Act) to insert two new powers:

---

\(^{437}\) Celina Truelove, 2018 Bill Review Submission 19, p. 1; Uniting Church in Australia, Synod of Victoria and Tasmania, 2018 Bill Review Submission 60, p. 9.

\(^{438}\) Uniting Church in Australia, Synod of Victoria and Tasmania, 2018 Bill Review Submission 60, p. 9.

• provision of voluntary assistance (accompanied by a grant of civil immunity), and
• compulsory provision of assistance to ASIO.

1.313 These new provisions and possible matters for further consideration are detailed below.

**Voluntary assistance and civil immunity**

**Synopsis**

1.314 The amendments enacted seek to encourage voluntary cooperation with ASIO in relation to the performance of its functions by offering immunity from civil liability to a person that voluntarily provides assistance to ASIO in accordance with a request made by the Director-General of Security, or in an unsolicited manner.

1.315 New section 21A of the ASIO Act provides that a person is not subject to any civil liability for conduct engaged in at the request of the Director-General of Security, or a delegated senior position-holder, as long as the conduct:

• is likely to assist ASIO in the performance of its functions, to the satisfaction of the Director-General or his or her delegate, on reasonable grounds, by way of certificate;\(^\text{440}\)
• does not involve the person committing an offence against a law of the Commonwealth, or a State or Territory, and
• does not result in significant loss of or serious damage to, property.\(^\text{441}\)

1.316 These powers are significantly similar to those contained in Schedule 1 of the amending Assistance and Access Act, (referred hereafter as the ‘industry assistance measures’), though are substantially broader as they are not limited to communications providers nor operate under the same decision-making criteria and oversight. For clarity, assistance provided under Schedule 5 is only able to be requested by ASIO (whereas industry assistance measures are available to ASIO, ASD, ASIS and designated interception agencies).

1.317 Amendments introduced and passed on 6 December 2018 include:

---

\(^{440}\) The certificate would be prima facie evidence of the facts certified in any proceedings to determine whether the civil immunities under the ASIO Act apply (ASIO Act, subsection 1A(9)).

\(^{441}\) ASIO Act, subsection 21A(8)—(Assistance and Access Act, Schedule 5, Item 2).
a request must be made in writing unless the Director-General is satisfied that:
- the request should be made as a matter of urgency; or
- making the request in writing would be prejudicial to security; or
- making the request in writing would be prejudicial to ASIO’s operational security, and

- the Director-General must inform the Inspector-General of Intelligence and Security within 7 days of making a request.

Possible matters for further consideration

1.318 The following matters were identified by stakeholders in the 2018 Bill Review as possible matters for further consideration, and were confirmed in submissions to the 2019 Act Review as ongoing matters (see footnotes). These matters were not addressed in the amendments introduced and passed on 6 December 2018.

Scope and limits of the grant of civil immunity

1.319 These new provisions represent a departure from the existing process for granting a statutory immunity for assisting ASIO. Further, the grant of a civil immunity has the effect of depriving third parties of a right of civil action. These two factors prompted stakeholders, including the IGIS, the AHRC and the Law Council, to recommend in the Committee’s 2018 Bill Review further consideration of the following:

- that a grant of civil immunity under new section 21A should only be made by the Attorney-General, in line with other pre-existing processes for the grant of civil immunity for participants in a special intelligence operations; and

- amendments requiring the decision-maker to consider proportionality and reasonableness of not only the request for voluntary assistance, but

---

442 ASIO Act, subsections 21A(2)-(2A) — (Assistance and Access Act, Schedule 5, Item 2).

also the provision of civil immunity (and the impact on third parties), and
greater clarity in the types of conduct that would be covered by the immunity (recommending that conduct that results in ‘pure economic loss’ and ‘harm or mental injury’ be excluded from the immunity).

Interaction with other powers available to ASIO

1.320 Stakeholders also sought clarification of the interaction between the provisions contained in Schedule 5 with ASIO’s other powers. For example, the IGIS, the AHRC and the Law Council identified the following as possible matters for further consideration:

- the amending Assistance and Access Act does not expressly exclude conduct that would require ASIO to obtain a warrant (or another form of authorisation) if it were to undertake itself. Absent of a clear and express exclusion, section 21A could provide a mechanism through which ASIO could effectively bypass standard practice to obtain warrants and authorisations for certain activities, and may allow ASIO to request a person to engage in conduct that ASIO would otherwise require a warrant to undertake, and
- further amendments that would provide clarity on the provision of civil immunity for industry assistance under Schedule 1 of the amending Assistance and Access Act and the provision of civil immunity under Schedule 5 under the same act. The civil immunity provisions in Schedule 5 are broader than its counterpart in Schedule 1 and the

---


decision-maker is not required to consider reasonableness, proportionality and the impact on third parties.\textsuperscript{447}

\textit{Transparency, accountability and oversight matters}

1.321 Although the provisions establish a legal avenue for voluntary assistance to be provided and are therefore not compulsive powers, the impact on third parties prompted stakeholders to identify a range of matters to improve the transparency, accountability and oversight of ASIO use of voluntary assistance requests. This included further amendments to provide for:

\begin{itemize}
\item a maximum statutory period for assistance requests and accompanying grants of civil immunity;\textsuperscript{448}
\item greater clarity in the authorisation of one-off requests and/or standing requests for assistance,\textsuperscript{449} or the express exclusion of standing requests;\textsuperscript{450}
\item specified grounds on which such requests may be varied or must be revoked;\textsuperscript{451} and
\item improved periodic reporting requirements to Parliament, including information related to:
\begin{itemize}
\item the number of times requests have been issued over the reporting period, and
\item the type of assistance requested and provided, and
\item any instances that are known to ASIO (if any) in which a person, requested to assist ASIO, engaged in conduct falling outside the scope of immunity, and if so,
\end{itemize}
\end{itemize}

\begin{footnotes}
\footnotetext[449]{Inspector-General of Intelligence and Security, 2018 Bill Review Submission 52, p. 56; Inspector-General of Intelligence and Security, 2019 Act Review Submission 1.1, p. 10.}
\footnotetext[450]{Australian Human Rights Commission, 2018 Bill Review Submission 47, p. 84; Law Council of Australia, 2019 Act Review Submission 4, p. 19.}
\footnotetext[451]{Law Council of Australia, 2018 Bill Review Submission 76, p. 51; Law Council of Australia, 2019 Act Review Submission 4, p. 19.}
\end{footnotes}
the quantum of any incurred loss (if known), or an estimated quantum.\textsuperscript{452}

**Compulsory assistance orders**

**Synopsis**

1.322 New section 34AAA empowers the Attorney-General, at the request of the Director-General of Security, to issue a compulsory assistance order requiring a ‘specified person’ to provide any information or assistance that is ‘reasonable and necessary’ to allow ASIO to access data held in, or accessible from, a computer or data storage device that is the subject of, or is found, removed or seized, under a separate ASIO warrant.\textsuperscript{453}

1.323 The penalty for non-compliance with such an order is five years imprisonment, or 300 penalty units ($63,000), or both.\textsuperscript{454}

1.324 This power is broadly similar to the assistance orders available under Schedules 2, 3, and 4 of the amending Assistance and Access Act.

1.325 The decision-making criteria that would be applied by the Attorney-General depends on the type of warrant or authorisation that ASIO seeks to give effect to. The amending Act distinguishes between foreign intelligence warrants and any other warrants or authorisations under the ASIO Act.

1.326 To issue an order that gives effect to **foreign intelligence warrant**, the Attorney-General must be satisfied on reasonable grounds that,

- ASIO’s access to the relevant data will be for the purpose of obtaining foreign intelligence relating to a matter specified in the warrant, \textit{and}
- the collection of foreign intelligence is in the interests of Australia’s national security, foreign relations or national economic well-being.\textsuperscript{455}

1.327 To issue an order that gives effect to warrants or authorisations **other than a foreign intelligence warrant**, the Attorney-General must be satisfied, on reasonable grounds, that the relevant access will substantially assist the


\textsuperscript{453} ASIO Act, section 34AAA—(Assistance and Access Act, Schedule 5, Item 3).

\textsuperscript{454} ASIO Act, subsection 34AAA(4)—(Assistance and Access Act, Schedule 5, Item 3).

\textsuperscript{455} ASIO Act, subsection 34AAA(2)(a)—(Assistance and Access Act, Schedule 5, Item 3).
collection of intelligence in respect of a matter that is important in relation to security. 456

1.328 Irrespective of the type of warrant or authorisation that ASIO seeks to give effect to in a compulsory assistance order, the amending Act establishes additional decision-making criteria. The Attorney-General must be satisfied, on reasonable grounds, that the specified person is:

- reasonably suspected of being involved in activities that are prejudicial to security, or
- the owner or lessee of the computer or device, or
- an employee of the owner or lessee of the computer or device, or
- a person engaged under a contract for services by the owner or lessee of the computer or device, or
- a person who uses or has used the computer or device, or
- a person who is or was a system administrator for the system including the computer or device, and
- the specified person has relevant knowledge of:
  - the computer or device or a computer network of which the computer or device forms or formed a part, or
  - the measures applied to protect data held in the computer or device. 457

1.329 Amendments introduced and passed on 6 December 2018 include:

- that the Director-General of Security may request a compulsory assistance order orally or in writing to the Attorney-General, though if requested orally, the Director-General must make a written record of the request within 48 hours; 458
- that a request must be accompanied by a statement setting out the particulars and outcomes of all previous requests; 459
- that if the Director-General is satisfied that the grounds on which a compulsory assistance order was made have ceased to exist, the Director-General must inform the Attorney-General, and if the Attorney-General concurs, the Attorney-General must revoke the order, 460 and

456 ASIO Act, subsection paragraph 34AAA(2)(b)—(Assistance and Access Act, Schedule 5, Item 3).
457 ASIO Act, subsections 34AAA(2)(c)-(d)—(Assistance and Access Act, Schedule 5, Item 3).
458 ASIO Act, subsections 34AAA(3A)-(3B)—(Assistance and Access Act, Schedule 5, Item 3).
459 ASIO Act, subsection 34AAA(3C)—(Assistance and Access Act, Schedule 5, Item 3).
460 ASIO Act, subsections 34AA(3D)-(3E)—(Assistance and Access Act, Schedule 5, Item 3).
• ASIO must provide a written report to the Attorney-General on the extent to which the action taken under the warrant has assisted ASIO in carrying out its functions, and the total number of requests and orders made must be included in ASIO’s annual report to the Minister.  

Possible matters for further consideration

1.330 The following matters were identified by stakeholders in the 2018 Bill Review as possible matters for further consideration, and were confirmed in submissions to the 2019 Act Review as ongoing matters (see footnotes). These matters were not addressed in the amendments introduced and passed on 6 December 2018.

Clarity, scope and limits compulsory powers

1.331 Noting the significant criminal penalty for failing to comply with an assistance order, stakeholders identified the following as possible matters for further consideration:

• the term ‘specified person’ may lack clarity, and it is ambiguous as to whether the term extends only to a natural person or bodies corporate;  

• that the enacted provisions do not require there to be a nexus between the prejudicial activities in which a specified person is involved and the security matter in respect of which the relevant warrant is issued;  

• that compulsory assistance orders (which, as enacted, may be issued to a person who is reasonably suspected of ‘being involved in’ activities prejudicial to security) be limited to persons ‘knowingly or intentionally involved in’ activities prejudicial to security, as the current threshold is ‘very low’; and

---

461 ASIO Act, subsections 34ZH(2) and 94(2BC) — (Assistance and Access Act, Schedule 5, Items 4, 5 and 6).


that the procedural requirements applied when a computer or data storage device is not on a premises in relation to which a warrant is in force (including a specified time period, the place at which a person must provide the information or assistance, and other relevant conditions) should apply irrespective of the physical location of a computer or storage device that is accessed.\textsuperscript{465}

Interaction with other powers available to ASIO

1.332 Stakeholders also sought clarification of the interaction between the provisions contained in Schedule 5 with ASIO’s other powers. For example, the IGIS and the Law Council identified the following as possible matters for further consideration:

- that additional amendments be introduced to clarify the interaction with ASIO’s compulsory questioning and detention and detention powers;\textsuperscript{466} and
- that additional amendments be introduced to clarify the use of a technical assistance notice issued by ASIO under Schedule 1 of the Assistance and Access Act (industry assistance measures) as opposed to ASIO’s specific powers to request a compulsory assistance order.\textsuperscript{467}

1.333 The IGIS and the Law Council recommended consideration of statutory safeguards to protect against the oppressive use of multiple coercive powers by ASIO.\textsuperscript{468} In a submission to the 2018 Bill Review, the IGIS suggested amendments that would require ASIO to provide the Attorney-General with

---


\textsuperscript{467} Inspector-General of Intelligence and Security, 2018 Bill Review Submission 52, p. 66; Law Council of Australia, 2018 Bill Review Submission 76, p. 54.

\textsuperscript{468} Inspector-General of Intelligence and Security, 2018 Bill Review Submission 52, p. 66; Law Council of Australia, 2018 Bill Review Submission 76, p. 55.
information when requesting a compulsory assistance order, including information about previous orders and requests for orders in relation to that same person. Amendments introduced and passed on 6 December 2018 included provisions to this effect.\footnote{ASIO Act, 34AAA(3C)—(Assistance and Access Act, Schedule 5, Item 3).}

**Potential for arbitrary detention**

1.334 While a person the subject of an assistance order may not be physically restrained, the new powers may, in effect, prevent that person from leaving a location prior to the completion of the designated assistance task, under pain of criminal penalty. This was considered as creating the potential to authorise detention by non-judicial officers. This prompted a number of stakeholders to suggest that the safeguards that are required under ASIO’s questioning warrants or questioning and detention warrants should be applied to an assistance order issued by the Attorney-General.\footnote{Australian Human Rights Commission, 2018 Bill Review Submission 47, pp. 81-82; Australian Human Rights Commission, 2019 Act Review Submission 56, p. 18; see also Inspector-General of Intelligence and Security, 2018 Bill Review Submission 52, p. 64; Inspector-General of Intelligence and Security, 2019 Act Review Submission 1.1, p. 4; Law Council of Australia, 2018 Bill Review Submission 76, p. 53.}

1.335 The risk that a compulsory assistance order may result in arbitrary detention was discussed by a number of stakeholders, with the AHRC making a detailed recommendation in the 2018 Bill Review for amendments to include:

- a maximum time limit on the period during which assistance must be provided;
- a right to contact a family member and a lawyer;
- an obligation on officers to explain the nature of the assistance order and what it requires;
- an obligation on officers to explain how to make a complaint to the IGIS or to challenge the making of the assistance order in court;
- a right to an interpreter, if necessary;
- an obligation to treat the specified person humanely and with respect for their human dignity; and
- sufficient safeguards to protect the interests of children in respect of whom an assistance order may be issued (for example: age limits,
notification of parents or guardians, and suspension of any obligations until a parent or guardian is present).⁴⁷¹

Privilege against self-incrimination

1.336 The AHRC and the Law Council echoed concerns regarding the privilege against self-incrimination, as discussed earlier in relation to the provisions contained in Schedules 2, 3 and 5 of the amending Assistance and Access Act.⁴⁷²


B. List of submissions

1 Inspector-General of Intelligence and Security
   ▪ 1.1 Supplementary to submission 1
   ▪ 1.2 Supplementary to submission 1

2 Commonwealth Ombudsman
   ▪ 2.1 Supplementary to submission 2

3 Communications Alliance, the Australian Industry Group (Ai Group), the Australian Information Industry Association (AIIA), the Australian Mobile Telecommunications Association (AMTA), the Digital Industry Group Inc (DIGI) and the Information Professionals Industry Association (IPTA)

4 Law Council of Australia
   ▪ 4.1 Supplementary to submission 4

5 Associate Professor Vanessa Teague and Dr Chris Culnane

6 Name Withheld

7 Paweł Glaz

8 Mr James Parsons

9 Mr Jake Bloom

10 Lee Sinclair

11 Independent Broad-based Anti-corruption Commission (IBAC)
12 Mr Justin Warren
13 Name Withheld
14 ASIO
15 Law Enforcement Conduct Commission
16 Department of Home Affairs
   ▪  16.1 Supplementary to submission 16
17 Mr Patrick Maher
18 Name Withheld
19 Name Withheld
20 MR Leon Zabakly
21 Australian Federal Police
22 Dr Joe Zucco
23 Mr Andrew Tyson
24 Dr Peter Serwylo
25 Name Withheld
26 Australian Information Industry Association
27 Investigative Commissions
28 Mr Peter Jardine
   ▪  28.1 Supplementary to submission 28
29 Internet Australia
30 Mr Derek Waters
31 Pirate Party Australia
32 Australian Criminal Intelligence Commission
33 Remi Forcet
34 Mr Peter Young
35 Kosmas Stergiou
36 BSA | The Software Alliance
37 StartupAUS
- 37.1 Supplementary to submission 37

38 Senetas Corporation Limited
39 Paul Wilkins
40 Corruption and Crime Commission
41 Name Withheld
42 Name Withheld
43 Mary Greene
44 Riana Pfefferkorn
45 Mr Charling Li
46 Paul Templeton
47 Assoc. Prof Boztas, Dr Clarke, Dr Hall, Prof Horadam & Prof Rao
48 FastMail Pty Ltd
50 International Civil Liberties and Technology Coalition
51 Dr Stephen Ranck
52 Dr Tom Allen
53 Access Now
54 Matt Cengia
55 Australian Civil Society Coalition
56 Australian Human Rights Commission
57 Assembly Four Pty Ltd
58 Mr Daithí Ó Gliasáin
59 Dr Les Kitchen
60 Ruby Australia
61 Mr Simon Dewar
62 Mozilla Corporation
63 Cyrus
64 Office of the Australian Information Commissioner
65 Mr Aleksa Sarai
66 Thoughtworks

Name Withheld

Name Withheld

Name Withheld

Name Withheld